حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى

دراسة حالة

د. فاتن سعيد بامفلح

مقدمة منهجية:

شغلت قضية أمن المعلومات في الآونة الأخيرة اهتمام أفراد المجتمع والمتخصصين، وأصبحت الصحف اليومية تطالعنا باستمرار بآخر المستجدات المتعلقة بتلك القضية، وعقدت العديد من المؤتمرات التي تركزت حول مناقشة ذلك الجانب الذي شغل الشخص العادي كما شغل المتخصص.
والواقع أن الحرص على حماية أمن المعلومات ليس بالموضوع الجديد على المكتبات؛ فقد كانت المكتبات ولازالت تحمي مجموعاتها بأساليب متعددة تتمثل في إجراءات الصيانة والتجليد والترميم وكذلك باستخدام النظم الأمنية التي تكفل حماية مجموعاتها من السرقة مثل ***access systems*** أو حراس الأمن على سبيل المثال.

وتراعي المكتبات باستمرار الموازنة بين أساليب الحماية المتبعة وبين إتاحتها لمصادر المعلومات وذلك على اعتبار أن تشديد الإجراءات الأمنية يؤدي إلى تقييد الاستخدام في بعض الأحيان ؛ فبعض المكتبات تمنع إعارة بعض مصادر المعلومات القيمة المتوافرة بها خوفاً من ضياعها وتستعيض عن خدمة الإعارة بخدمات أخرى لإتاحة استخدام تلك المصادر.
وقد ظهرت في المكتبات أساليب حديثة ومختلفة لحماية أمن المعلومات في عصر شبكات المعلومات التي أصبحت أشكال التهديد فيها مختلفة عما كانت عليه في السابق وبالتالي فإن أساليب الحماية اختلفت أيضاً.

وتبرز الحاجة للمحافظة على أمن المعلومات بدرجة أكبر في شبكات المعلومات عنها عند التعامل مع أجهزة الحاسب الشخصية التي تعمل بصورة مستقلة؛ وذلك بسبب تعدد أوجه الخطر التي تواجهها المعلومات عند إتاحتها من خلال شبكات ؛ حيث يمكن معها إلحاق الضرر بالمعلومات والأجهزة عن بعد دون الحاجة إلى التواجد في نفس المكان. ويأخذ تهديد أمن المعلومات أكثر من شكل إلا أنه من الممكن إجمالها في الآتي:

١. تعرض الشبكة ومواردها لعمليات الاختراق والتجسس والسرقة
٢. تعرض المعلومات للإتلاف أو التحريف أو التخريب.

وفي هذه الدراسة تستعرض الباحثة أساليب حماية أمن المعلومات المتبعة في المكتبات في ظل استخدامها لشبكات المعلومات، وتتناول تطبيق تلك الأساليب على شبكة المكتبات بجامعة أم القرى للتعرف على مدى كفاية تلك الأساليب المتبعة فيها لتحقيق أمن المعلومات.

وتهدف الدراسة إلى قياس مدى كفاية الإجراءات الأمنية المطبقة على شبكة مكتبات جامعة أم القرى، والتعرف على مواطن القوة وجوانب القصور فيها وذلك في سبيل تطوير تلك الإجراءات وزيادة إحكامها.

وتركز الدراسة من الناحية الموضوعية على الجوانب المتعلقة بحماية أمن المعلومات في الشبكات ومدى تطبيقها على شبكة مكتبات جامعة أم القرى في زمن إجراء هذه الدراسة والمتمثل في عام ١٤٢٢/١٤٢١ هـ سواء كان ذلك في المكتبة المركزية للطلاب أم في المكتبة المركزية للطالبات.

وتنقسم الدراسة إلى قسمين أحدهما نظري يعتمد على المنهج الوثائقي في جمع المعلومات من الإنتاج الفكري المكتوب حول الموضوع، والقسم الثاني يمثل دراسة حالة لشبكة المعلومات بجامعة أم القرى حيث أجرت الباحثة دراسة وصفية على الشبكة القائمة في عمادة شئون المكتبات تناولت فيها جوانب الحماية المطبقة وكيفية تطبيقها، وقد استعانت الباحثة باستمارة لجمع المعلومات (ملحق ١) تم إرسالها الى سعادة عميد شئون المكتبات ، كما اعتمدت الباحثة على بعض الوثائق الرسمية المكتوبة والمرتبطة بمجال الدراسة، بالإضافة إلى إجراء بعض المقابلات مع كل من مدير المكتبة المركزية، ونائب رئيس قسم الحاسب الآلي بالمكتبة المركزية، والمسئول عن الشبكات في مركز المعلومات والحاسب الآلي والتطوير الجامعي بالجامعة.

وتجيب الدراسة على التساؤلات التالية:

١. ما الإجراءات الأمنية المتبعة في شبكة المعلومات بعمادة شئون المكتبات بجامعة أم القرى؟
٢. ما الإجراءات الأمنية التي تفتقدها شبكة المعلومات بالعمادة ؟
٣. هل تعد الإجراءات الأمنية التي تتبعها العمادة كافية؟
٤. كيف يمكن تطوير الأساليب المتبعة لحماية أمن شبكة معلومات العمادة؟

وقد ظهرت العديد من الدراسات السابقة التي تناولت موضوع أمن المعلومات ومن بينها دراسة ***Rowley -J*** [(١)] الصادرة عام ١٩٩٥م والتي تناولت الجوانب التي تهدد أمن المكتبات والمعلومات سواء في شكلها التقليدي أم في غيره بما في ذلك نظم الحاسبات الآلية، واستعرضت الدراسة السياسات الأمنية ومكوناتها ،كما تناولت تأثير التهديد وفقدان الأمن على المكتبات، مشيرةً إلى أنواع المخاطر التي تتعرض لها.

وفي عام ١٩٩٧م صدرت دراسة ***Cervone F*** [٢] التي تناولت الجوانب المتعلقة بأمن شبكة المعلومات في نظام ***Illinois ILLInet online*** بعد إدخال الفهرس الموحد المباشر ***online union cataloging*** ، وقد أشارت الدراسة الى المفاهيم العامة المتعلقة بأمن الشبكات، كما تناولت بعض الاعتبارات الفنية التي تراعى على مستوى محطات العمل وأجهزة الخادم الخاصة بالشبكات المحلية ***LAN server*** وأجهزة الخادم الخاصة بالويب ***web server*** ، كما تعرضت الدراسة للجوانب المتعلقة بتفاعل الأفراد مع الحاسبات على اعتبار أنها تمثل جانباً من الجوانب الهامة التي ينبغي مراعاتها لتطبيق النظام الأمني.

وفي عام ١٩٩٨م استعرضت دراسة أشرف الغنيمي[٣] الطرق المتعددة لانتهاك أمن المعلومات في نظم الحاسب الآلي وأساليب الحماية منها، وأوضحت المخاطر التي تهدد أجهزة الحاسب بما في ذلك الفيروسات وكيفية تحقيق الحماية منها، وقد خصصت الدراسة فصلاً للجوانب المتعلقة بأمن شبكات المعلومات والمخاطر الأمنية التي تتعرض لها.

وفي عام ٢٠٠٠م صـــدرت دراســـة لكـــل من ***Hawkins-S*** و ***Yen D-C***و ***Chau D-C*** [٤] تناولت الطرق المتعددة لتحقيق أمن البيانات للهيئات المرتبطة بشبكة الإنترنت، سواء كان ذلك عند نقل تلك البيانات عبر الشبكة أو عند تخزينها؛ بما في ذلك التشفير، والحوائط النارية، والشبكات الخاصة.

وفي العام نفسه صدرت دراسة لحسن طاهر داود[٥] تناولت مفهوم أمن المعلومات وكيفية تحقيقه سواء على مستوى تطبيق الأمن المادي للمنشآت أو للأجهزة أو للأفراد ، أم من خلال تشفير البيانات، أم ما سوى ذلك من أساليب، كما تناولت جرائم الحاسب المختلفة وفيروسات الحاسب. وأوضحت الدراسة كيفية تحقيق أمن التطبيقات، وأمن قواعد البيانات، وأمن شبكات نقل المعلومات، وأمن شبكات إنترانت المحلية، وأمن شبكة الإنترنت.

المخاطر التي تتعرض لها الشبكات:

هناك أساليب عديدة تتبع لحماية الشبكات منها ما يخص التجهيزات المادية ومنها مـــا يخـــص البرامج والبيانات ، منها ما يتم محلياً في موقع تجهيزات الشبكة ومنها ما يتم لحماية الشبكة خـــلال الاتصال عن بعد. وقبل الإشارة الى أساليب الحماية ينبغي التعرف على أبرز المخاطر التي تتعرض لها الشبكات، وتتمثل في الآتي:

١. اقتحام الهاكرز ***Hackers**** والكراكرز ***Crackers***** للشبكة مما يؤدي إلى تفشي أسرار العمل والعاملين، أو تخريب البيانات وإتلافها، وذلك على اعتبار أن وصول أشخاص غير مصرح لهم إلى ملفات البيانات قد يعرض البيانات للتغيير أو التعديل أو المسح وبالتالي يؤدي الى تحريف البيانات أحياناً والى سرقتها في أحيان أخرى.

٢. تعليق شخص لمعدات معينة على الكابلات بغرض التنصت عليها.

٣. مراقبة خطوط الهاتف والتجسس على مستخدمي الشبكة.

٤. إقحام الفيروسات للشبكة سواء كانت فيروسات مزعجة فقط أم مدمرة تعرض أجهزة الشبكة وبياناتها للتلف أو الفقد.

٥. إطلاع الأشخاص المصرح لهم باستخدام الشبكة على معلومات غير مصرح لهم بالاطلاع عليها.

٦. التشويش على الإشارات المنقولة عبر الكابلات.

٧. تعطيل أحد الأشخاص لنظام الأمن الخاص بالشبكة أو كشفه لإجراءات الحماية المتبعة.

وان كان من الممكن تعرض الشبكة للمخاطر السابقة وغيرها سواء تم استخدامها من نفس الموقع أم عن بعد، إلا أن هناك مخاطر أخرى تتعرض لها الشبكة في الموقع نفسه فقط، في حين تؤثر على استخدامها سواء عن قرب أم عن بعد، وتتمثل في الآتي:

١. سرقة الأقراص المحملة عليها البيانات مما يودي الى فقدان البيانات وتفشي أسرار عن الأشخاص وعن العمل.

٢. تخريب الأجهزة سواء بقصد أو بدون قصد مما يؤدي إلى انقطاع الخدمة.

٣. إغلاق أجهزة الخادم مما يؤدي إلى توقف الشبكة عن العمل.

---

* الهاكرز ***Hackers*** : (هو الشخص الذي حقق مهارة تقنية عالية ويجد متعة خاصة في الدخول غير المشروع الى أنظمة الحاسبات الكبيرة عبر الشبكات، وذلك لمجرد سعادته بالتغلب على التحدي المتمثل في التغلب على نظام الحماية والأمان الذي تستعمله الشركة)(٦).

** الكراكر ***Cracker*** : شخص يخترق النظم الأمنية بغرض سرقة أو إفساد البيانات، أي أن هدفه تخريبي أو إجرامي(٧).

٤. تعرض المكان للحريق مما يؤدي إلى فقدان البيانات وتلف الأجهزة.

٥. تعطل مولد الطاقة مما يؤدي إلى توقف الشبكة وانقطاع الخدمة.

٦. تعطل مكونات الشبكة مثل الأقراص الصلبة على سبيل المثال.(٨)

ويتضح مما سبق أن ما تتعرض له الشبكة من مخاطر في الموقع نفسه يفوق ما يمكن أن تتعرض له عن بعد، وعلى الرغم من ذلك إلاّ أن إلحاق الأذى بالشبكة عن بعد يعد أكثر سهولة وأكثر خطورة من إلحاق الأذى بها في الموقع نفسه وذلك للاعتبارات التالية[٩]:

١. أن الشخص يمكنه الوصول إلى المعلومات عن بعد دون الحاجة لتجاوز الأسوار والأبواب المغلقة أو الحراسة التي قد تخصص في موقع تواجد أجهزة الشبكة.
٢. يمكن رؤية المستخدم في الموقع وكشف ما يفعله بالأجهزة وما يفعله بالبيانات بسهولة، أما في الاتصال عن بعد فلا يمكن معرفة الشخص المتصل بالشبكة حيث أن كل ما يظهر هو الحساب ***account*** الذي يستخدمه، وهو الأمر الذي لا يعبر عن المستخدم الفعلي للشبكة.
٣. استخدام كابلات غير محمية للاتصال بالشبكة لربط المتصل عن بعد يؤدي إلى صعوبة حماية الشبكة نظراً لصعوبة منع خط الهاتف العمومي من تعرضه للمراقبة في نقطة معينة خلال الاتصال بالشبكة.

وهناك أساليب عديدة تتبع لحماية الشبكة والمحافظة على أمن المعلومات فيها، ولابد من مراعاة تطبيق بعض تلك الأساليب عند التخطيط للشبكة وإنشائها، في حين يراعى البعض الآخر عند اختيار البرامج، هذا إلى جانب الأساليب المرتبطة بالقائمين على الشبكة ومستخدميها. وفيما يلي إيضاح لأبرز الأساليب المتبعة لحماية الشبكات:

أولاً: أساليب الحماية الفيزيائية ***physical security***:

تتمثل في اختيار المكان الملائم والتجهيزات الأكثر حفاظا على الأمن. ولتحقيق هذا المستوى من الحماية لابد من مراعاة الآتي[١٠]:

١. تخصيص غرف مغلقة لحفظ أجهزة خادم الشبكة ***servers*** في حالة وضعها في غرف مركزية، أما إذا لم يكن ذلك متاح فلابد من حفظ أجهزة الخادم ضمن غرف الإداريين.
٢. اختيار الكابلات الأكثر حماية للمعلومات كلما كان أمن المعلومات ضرورياً للهيئة ، وتتمثل في كابلات الألياف الضوئية ***Fiber Optics*** وذلك على اعتبار أنها تلغي الإشعاع الثانوي للكابلات وبالتالي تمنع التنصت على البيانات خلال نقلها عبر الكابلات.
٣. تركيب تمديدات وكابلات الشبكة في أماكن محمية غير معرضة لوصول غير المختصين لها، بحيث لا تكون ظاهرة للعيان، فيمكن على سبيل المثال تمريرها عبر الجدران وفوق السقف

وتحت الأرض حتى تتم حمايتها قدر الإمكان من أجهزة التنصت وكذلك حمايتها من التعــرض للقطع أو الثني في حالة وضعها تحت قطع المفروشات الثقيلة.

٤. استخدام الكابلات المغلفة وذلك لتقليل الإشعاع الثانوي المنبثق من خلالها، ويمكن إضافة أكثر من غلاف عليها لمنع الإشعاع نهائياً.

٥. تأمين النوافذ والفتحات الأخرى الموجودة في غرفة الخادم خصوصاً إذا كانت قريبة مـــن الأرض.

٦. تأمين الأبواب والمنافذ الأخرى كالنوافذ باستخدام أجهزة إنذار آلية تقوم بتشغيل أجراس للتنبيه في حالة دخول أشخاص للموقع في غير أوقات العمل.

٧. توفير وسائل مراقبة للموقع مثل الدوائر التلفزيونية المغلقة، وذلك لإتاحة المراقبـــة بعـــد ساعات الدوام .

ثانياً: ضبط الوصول إلى الشبكة وإتاحة مواردها *access control system*:

من الضروري ضبط الوصول إلى الشبكة لحمايتها من التعرض لعمليات الاقتحـــام ،ولا يقتصـــر الأمر هنا على حماية الشبكة من الاقتحام من قبل أشخاص غير مصرح لهم نهائياً بالـــدخول إليهـــا واستخدام مواردها، ولكن يتجاوزه إلى حمايتها أيضاً من محاولة دخول أشخاص مصـــرح لهـــم إلى ملفات ومصادر غير مصرح لهم باستخدامها. ولتحقيق ذلك لابد من تخصيص اسم أو رقم تعريـــف لكل مستخدم للشبكة ***User ID*** وكلمة مرور ***Password*** حيث تعد هذه هـــي الخطـــوة الأولى المتبعة لمنع اقتحام الشبكات يتبعها التحقق من أن المستخدم لديه حقوق ممارسة ما يريد ممارسته على موارد الشبكة مثل حق الإنشاء للملفات والفهارس، أو حق المسح والاستعراض أو التغـــيير أو الفتح والقراءة أو الكتابة..الخ ويمكن أن يمنح المستخدم حقاً أو اكثر من تلك الحقوق حسب تصنيفه، كما يمكن تخصيص صفات للملفات نفسها مثال: ملف للقراءة فقط، ملف للقراءة والكتابة، ملـــف غير قابل للإلغاء، ملف غير قابل للنسخ..وهكذا...(١١). وبذلك يتضح أن هناك شـــكلين متـــاحين لضبط إتاحة الوصول إلى الشبكة وهما على النحو التالي:

أ. **إتاحة على مستوى مشاركة:**

يتم وفقاً لهذا الشكل تحديد اسم تعريف وكلمة مرور لكل مصدر متاح للمشـــاركة علـــى الشبكة، ويتم استخدام نفس الاسم وكلمة المرور من قبل كل مستقبل يريد الوصـــول الى هـــذا المصدر.

ويحدد لكل مصدر مستوى الإتاحة الخاص به مثال: قراءة فقط، أو كتابة فقط ، أو مشاركة كاملة...الخ

ويعيب هذا الشكل انه يتطلب من المستخدم تذكر كلمات مرور متعددة كل منها خاصة بمصدر من مصادر المشاركة، وبذلك فإنه يصعب استخدامه كلما زاد عدد موارد الشبكة لأن ذلك يعني زيادة عدد كلمات المرور، وهو بذلك أكثر ملاءمة للشبكات الصغيرة، ويفيد في الاستخدام مع شبكات النظير للنظير ***peer to peer***. ومن عيوبه أيضاً أنه من السهل تفريط الشخص بكلمة المرور الخاصة بالمورد وتعريف آخرين بها حيث أنها ليست كلمة المرور الخاصة به شخصياً.

ب. إتاحة على مستوى مستخدم:

يتم وفقاً لهذا الشكل تحديد اسم تعريف وكلمة مرور لكل مستخدم ، ويتم تحديد لائحة المستخدمين إلى المورد أو الموارد المصرح لهم باستخدامها، وتتم إضافة أي مستخدم جديد لتلك اللائحة أو حذف مستخدم منها عند الحاجة لذلك، ويمكن تحديد مستوى الإتاحة الممنوح لكل مستخدم أو مجموعة مستخدمين بحيث يحدد ما إذا كان مصرح له بالقراءة فقط أم التعديل أم الإلغاء أم غير ذلك.

ويتميز هذا الشكل بأنه لا يتطلب من المستخدم أن يتذكر سوى كلمة مرور واحدة لتسجيل الدخول إلى موارد الشبكة، وكذلك من الصعب على أي شخص أن يمنح كلمة مرور خاصة به لشخص آخر لاستخدامها كما هو الحال بالنسبة لمستوى المشاركة ومن هنا فإن هذا الشكل يحقق درجة تحكم في تنظيم الموارد ذات مستوى أعلى من مستوى المشاركة[١٢].

ولابد على المستخدم من مراعاة القواعد المتبعة لحماية كلمة المرور وذلك لضمان عدم كشفها من قبل الآخرين، ومن تلك القواعد ما يلي:

أ. تغيير كلمة المرور بانتظام، على أن يراعى عدم الإبقاء عليها اكثر من ٣٠ يوماً دون تغيير.

ب. عدم استخدام كلمات من السهل على الآخرين تخمينها مثل الكلمات القصيرة والمألوفة والمرتبطة بأمور شخصية مثل اسم الشخص أو أسماء أبنائه أو المقربين إليه أو تاريخ ميلاده أو الفريق المفضل لديه، أو الكلمات المرتبطة بمجال عمله... وما شابه ذلك.

ج. عدم استخدام كلمات مرور قصيرة ، حيث ينصح بأن يصل عدد حروفها إلى ١١ محرف[١٣].

وقد ظهرت أساليب متعددة للتحقق من هوية المستخدم ومن ذلك حفظ كلمات المرور في غير شكلها المطبوع، ومن الأساليب المتبعة لذلك ما يلي:

- **استخدام البطاقات الذكية *Smart Cards***

هي بطاقات تختزن فيها المعلومات مثل اسم الشخص وبياناته وكلمة المرور الخاصة به على شريط مغناطيسي وعند رغبة الشخص في الدخول للشبكة أو استخدام مواردها فعليه تمرير البطاقة خلال ماسح رقمي يعمل على قراءة البيانات المختزنة عليها ومضاهاتها بالمختزنة في النظام فإذا تطابقت يسمح له بالدخول والاستخدام.

- **تقنية البيولوجيا الإحصائية *biometric devices***

هي تقنيات تعرف بهوية المستخدم بشكل منفرد عن طريق بصمة إصبعه أو بصمة يده أو بصمة صوته أو غير ذلك من معرفات فردية لا يمكن أن تتشابه بين الأشخاص ، وتحول تلك التقنيات تلك المعرفات إلى إشارات رقمية تحفظ في ملف لكلمات المرور، وعند محاولة الشخص الدخول الى الشبكة واستخدام مواردها يقوم بإظهار بصمة يده أو إصبعه أو عينه أو صوته للماسح ***scanner*** فيتم التعرف على البصمة وتحويلها الى إشارات رقمية ومقارنتها بالنسخة المختزنة في النظام فإذا تطابقت معها بدرجة كافية يسمح النظام للشخص بالدخول الى الشبكة أو المورد المطلوب[١٤].

وتسمح نظم تشغيل الشبكات الحديثة بمراقبة النظام ***monitoring*** ومتابعة نشاطات المستخدم على الشبكة ومواردها من خلال اتباع سياسة التدقيق ***logging security*** التي تتيح معرفة من يفعل ماذا على الشبكة؟ وذلك بمتابعة عناصر متعددة على النحو التالي:

أ. تتبع نجاح أو فشل كل محاولة من محاولات دخول كل مستخدم للشبكة.

ب. تتبع نجاح أو فشل كل محاولة من محاولات المستخدم للوصول للملفات والموارد الأخرى على الشبكة.

ج. تتبع نجاح أو فشل كل ممارسة من كل مستخدم للحقوق الممنوحة له.

د. تتبع نجاح أو فشل كل محاولة من محاولات التعديل في سجلات المستخدمين والمجموعات .

ه. تتبع نجاح أو فشل كل محاولة لتعديل سياسة الحماية بما في ذلك تعديل حقوق المستخدمين أو سياسة التدقيق أو ما سوى ذلك.

و. تتبع نجاح أو فشل كل محاولة لإعادة تشغيل النظام أو إقفاله.

ز. تتبع نجاح أو فشل كل محاولة معالجة للنظام مثل استخدام التطبيقات وما سوى ذلك[١٥].

ويتضح مما سبق أن نظام التدقيق يعطي مؤشرات لمحاولات اقتحام الشبكة واختراق أمنها، ولابد من ضبط هذا النظام بحيث تتم مراجعته كل فترة زمنية (يوم أو أسبوع) وإلغاء المعلومات القديمة بعد تخزينها في ملفات للرجوع إليها عند الحاجة[١٦].

ثالثاً: تشفير البيانات Encryption:

يعرف التشفير بأنه عملية تشكيل البيانات باستخدام خوارزمية ***algorithm*** معينة تسمى المفتاح ***key*** تصبح بها غير قابلة للقراءة إلا بعد استخدام الخوارزمية لفكها. ويتم عادة تشفير البيانات قبل إرسالها عبر الشبكة وذلك لضمان سلامة وصولها دون التعرض لأي عمليات تجسس أو تحريف لمضمونها، على أن يتم فك الشفرة لدى مستقبل الرسالة باستخدام مفتاح فك الشفرة [١٧].
وينبغي الحرص على تشفير البيانات عند الرغبة في إرسالها عبر الشبكة، سواء كانت تلك البيانات كلمات مرور أم أرقام بطاقات الائتمان أم رسائل بريد إلكتروني أم ملف أم غير ذلك. وكلما كانت سرقة البيانات تمثل خطورة كلما كانت هناك ضرورة اكبر لتشفيرها.
ويمكن قراءة البيانات المشفرة واضحة من قبل أي شخص يعرف مفتاح الشفرة. ويتم في بعض الأحيان كسر الشفرة من قبل آخرون والتعرف على مفتاحها، وكلما كان مفتاح الشفرة طويل كلما كان من الصعب كسرة ، فعلى سبيل المثال يسهل كسر مفتاح شفرة طوله ٨ بت في حين أنه من الصعب كسر شفرة بطول ١٢٨ بت. وهناك شفرات بطول ٤٠ بت وهي شائعة الاستخدام في العالم، وكذلك شفرة بطول ٥٦ بت كالمستخدمة من قبل الحكومة الأمريكية والمعتمدة على نظام ***(DES) Data Encryption Standards*** . وتمنع الحكومة الأمريكية الشركات من إنتاج برامج تشفير تستخدم شفرة أكثر من طول ٤٠ بت إلا في نطاق محدود وذلك لاحتياطات أمنية [١٨].

أنواع التشفير:

للتشفير نوعان هما:

أ. **التشفير المتماثل *Symmetric Encryption*** :

يستخدم فيه المفتاح نفسه للتشفير وفك الشفرة، وبذلك فإن المفتاح يكون معروفاً من قبل كـــل من مرسل الرسالة ومستقبلها، ولا يتم إرسال المفتاح مع الرسالة ولكنه يرسل بوسيلة أخرى.

وحرصاً على حماية سرية المفتاح وعدم اطلاع الغير عليه عند إرساله إلى مستقبل الرســـالة، فقـــد استخدمت كتب للأكواد ***secure code book*** ، وتتضمن قائمة بمفاتيح التشفير التي يجـــب ان تستخدم بطرق محددة، فعلى سبيل المثال فإن أي رسالة ترسل يوم الأربعاء يتم استخدام مفتـــاح***a*** لفك شفرتها. وتفقد كتب الأكواد قيمتها إذا ما سرقت لأن ذلك يعني كشف المفتاح من قبل الغير.

ب. **التشفير غير المتماثل *Asymmetric Encryption*** :

يستخدم فيه مفتاحان لكل مستخدم؛ أحدهما مفتاح عام ***public key*** معروف مـــن قبـــل الآخرين حيث يسجله الشخص عادة مع توقيعه على البريد الإلكتروني ***e-mail signature*** وفي حالة الرغبة في إرسال رسالة مشفرة إلى ذلك الشخص يتم استخدام ذلك المفتاح العام لكتابة الشفرة، أما لفكها فيستخدم مفتاح خاص ***private key*** لا يعرفه سوى المستقبل نفسه، ويستخدمه لفك الشفرة المكتوبة باستخدام مفتاحه العام.

وعلى الرغم من ارتباط كل من المفتاح العام والخاص ببعضهما إلا أن أي منهما لا يدل على الآخر مطلقاً، فلا يمكن الاستدلال على المفتاح الخاص من خلال العام أو العكس[١٩].

وهناك طرق متعددة للتشفير تتراوح في درجة تعقيدها؛ فقد تكون سهلة للغاية ولا تتعدى فكرة الاستبدال كما هو الحال في "شفرة قيصر" التي تمثل في أبسط صورها استبدال كل حرف في الأبجدية بحرف آخر وفقاً لمفتاح الشفرة المحدد والذي قد يكون رقم (٣) على سبيل المثال وبالتالي يتم استبدال كل حرف من حروف النص الأصلي بثالث حرف يليه في الأبجدية، ويقوم مستقبل الرسالة بفك الشفرة باستخدام نفس المفتاح الذي يمثل رقم (٣) في هذا المثال فيعيد الحروف الأصلية للرسالة.

وقد تم تطوير طريقة الاستبدال حتى تصبح أكثر تعقيداً وبالتالي يصبح كسرها أمراً أكثر صعوبة فاستخدمت طريقة استبدال الحرف الأول في الأبجدية بالحرف الذي يليه واستبدال الحرف الثاني بالحرف الذي يليه بحرفين واستبدال الثالث بثالث حرف يليه في الأبجدية ثم نعود لنستبدل رابع حرف بأول حرف يليه وهكذا...ووفقاً لهذا المثال فإن حرف الألف يستبدل بحرف الباء ، وحرف الباء يستبدل بالثاء، أما التاء فيستبدل بالحاء، في حين يستبدل حرف الثاء بالحرف الذي يليه وهو الجيم وهكذا...

وقد تكون الشفرة أكثر قوة وتعقيداً من فكرة الاستبدال كما هو الحال بالنسبة لأســـلوب تشـــفير البيانات القياسي ***Data Encryption Standards (DES)*** وهو أيضاً أســـلوب مـــن

أساليب استخدام المفتاح السري كما هو الحال بالنسبة للطريقتين السابقتين، وهذا الأسلوب هو المتبع من قبل الحكومة الأمريكية منذ عام ١٩٧٧م حيث اعتمدته بعد أن أجرت عليه تعديلات كثيرة بعد أن طورته في منتصف السبعينات شركة **IBM**.

وهناك أساليب أخرى للشفرة تعتمد على استخدام المفتاح العام **public key** منها نظام خوارزمية **Rivest,Shamir,Adleman (RSA)** للتشفير الذي ظهر عام ١٩٧٨م بواسطة ثلاث علماء هم رايفست وشامير وأدلمان. ويمكن الحصول على هذا النظام في شكل رقيقة **chip** يتم تركيبها في الحاسب الآلي، وتعمل على التشفير وفك الشفرة ، ولكن هذه الرقائق غير متاحة في كل دول العالم لاعتبارات أمنية[٢٠].

رابعاً: استخدام الحوائط النارية **Firewalls** :

الحائط الناري هو عبارة عن برنامج **software** أو عتاد **hardware** لحماية موارد الشبكة من مستخدمي الشبكات الأخرى. وتستخدم في حالة ارتباط الشبكة بشبكات واسعة **WAN**، وتعمل على منع المستخدمين الخارجيين من الوصول الى موارد الشبكة وبياناتها الخاصة[٢١].

وتمثل الحوائط النارية نظاماً أمنياً قد يقتصر على برنامج فقط يحمل على جهاز الخادم **server**، وقد يتجاوز ذلك أحياناً ليشمل حلولاً متكاملة تضم برنامج وأجهزة مخصصة يعمل عليها ومزودة بمودمات وبطاقات شبكات[٢٢].

وتعمل هذه الحوائط كفلتر أو مصفاة لاختبار كل محاولات الدخول للشبكة بحيث لا تسمح بالمرور إلا للاتصالات المسموح بها وتحجز كل ما عدا ذلك، وبذلك فإن دورها يشتمل الآتي:

١. فحص كل الأنشطة الداخلة إلى الشبكة من مصادر خارجية مثل الإنترنت أو الشبكات الواسعة **WAN** الأخرى.
٢. ضبط المنافذ **ports** المستخدمة بحيث يسمح باستخدام منافذ معينة لأغراض معينة؛ فعلى سبيل المثال إذا أتيح منفذ **21** لنشاط **FTP** فإنه لن يسمح بدخول **FTP** من منفذ آخر.
٣. رفض وصول أنشطة معينة من عناوين محددة[٢٣].

ويراعى في الحوائط النارية إلا تؤدي إلى إعاقة عمل مستخدمي الشبكة الفعليين حتى تؤدي الغرض منها على النحو المطلوب. وتعمل حوائط النار عادةً وفقاً لقواعد أمنية محددة يضعها مدير الشبكة الداخلية؛ كأن تسمح سياستها بالمرور من داخل الشبكة إلى البيئة الخارجية (الشبكة

الخارجية) بحرية في حين لا تسمح في المقابل بالمرور من الخارج إلى الداخل نهائياً أو تسمح به في حدود معينة كالسماح بالمرور لمستفيدين دون غيرهم، أو لمواقع دون غيرها أو ما شابه ذلك.

وهناك اتجاهان متبعان لضبط الفعل التلقائي ***default*** للحوائط النارية وهما على النحو التالي:

١) أن يكون الفعل التلقائي ***default*** هو الإباحة : ويقصد به أن كل ما لم يُنص على منعه فهو مباح.

٢) أن يكون الفعل التلقائي ***default*** هو المنع : ويقصد به أن كل ما لم يُنص على إباحته فهو ممنوع.

ويعد الاتجاه الثاني هو الأكثر إحكاماً للأمن، أما الأول فهو الأفضل بالنسبة للمستفيدين[٢٤].

وقد تتم الإباحة أو المنع بناءً على اسم المستخدم وكلمة المرور، أو عنوان ***IP***، أو رقم هاتف المتصل في حالة السماح بالدخول عبر اتصال ***dial in*** . وتجدر الإشارة إلى أنه على الرغم من أن الحوائط النارية تحمي الشبكة ممن هم خارج حدودها، كما يمكن أن تحمي جزءاً من الشبكة بعزلة عن باقي أجزائها، إلا أنها على الرغم من ذلك لا تحمي من خطر العاملين داخل الحوائط[٢٥].

وتصدر تقارير عن الحوائط النارية تبين نشاطها خلال فترة معينة مما يتيح متابعة محاولات اختراق الشبكة،وللتأكد من استمرار فعالية الحوائط النارية فإنه يجب تحديثها بصورة منتظمة.

ويصمم بعض العتاد ***hardware*** خصيصاً ليكون حائطاً نارياً فقط بحيث لا يؤدي وظائف أخرى على الشبكة؛ ومن ذلك ***black box system***، وقد تكون أجهزة تقوم بوظائف أخرى إلى جانب عملها كحوائط نارية لتحميل برامج حوائط النار عليها؛ ومن ذلك:

١) الراوتر ***router*** :وتؤدي أبسط ما يمكن أن تقدمه أنواع الحوائط النارية حيث تعمل كحاجز مصفي ***filtering firewalls*** يقوم بفحص عناوين المعلومات ***IP addresses*** وتحديد ما يسمح بمروره وما يمنع مروره منها.

٢) البروكسي أو الوكيل ***proxy*** : ويطلق عليها حوائط نار البروكسي ***proxy firewalls*** وتعمل على فحص المعلومة قبل مرورها من الشبكة الخارجية إلى الشبكة الداخلية[٢٦].

خامساً: برامج الحماية ضد الفيروسات ***Virus protection software***:

الفيروس ***virus*** هو برنامج مصمم لتحقيق الهدفين التاليين:

أ. الانتشار من خلال إنشاء نسخ من نفسه وكل نسخة تنسخ نفسها تلقائياً وتنتشر في المزيد من أجهزة الحاسب الآلي.

ب. إلحاق الأذى بالبرامج أو الأجهزة.

وقد لا يتجاوز تأثير الفيروس بعد انتشاره أداء عمل غير ضار كعرض رسالة ساخرة على سبيل المثال، في حين يلحق في أحيان أخرى ضرراً بالغاً بالحاسبات مثل مسح المعلومات من قرص التخزين، أو تشتيت البرامج، أو حذف التطبيقات، أو خلق أخطاء غير مفهومة، أو تخريب القرص الصلب[٢٧].

أنواع الفيروسات:

يمكن تقسيم الفيروسات الى نوعين رئيسيين هما فيروس الماكرو ***Macro virus*** ، وفيروس قطاع التشغيل ***Boot sector virus*** وكل من النوعين يختلف في طريقة إصابته لأجهزة الحاسب، كما يختلف في طريقة تأثيره عليها.

أ. **فيروس الماكرو *Macro virus***

هو عبارة عن برنامج صغير مكتوب باستخدام لغة برمجة داخلية للتطبيقات مثل فيجوال بيسيك للتطبيقات ***Visual Basic Application (VBA)***، ويقوم فيروس الماكرو على عمل نسخ من نفسه بداخل الملفات المنشأة باستخدام البرامج التطبيقية مثل برامج ***WinWord***، ***Excel***. ويعمل الماكرو عند فتح أو إغلاق الملف أو عند حفظ ملف أو أثناء تشغيل البرنامج.

ب. **فيروس قطاع التشغيل *Boot sector virus***

تتركز هذه الفيروسات في قطاع التشغيل لأقراص الحاسب الآلي، ولا تحتاج كالنوع السابق الى ملفات للدخول إلى الجهاز حيث يصاب الجهاز بالفيروس عند محاولة تشغيله من خلال قرص مصاب بالفيروس. وبتشغيل جهاز الحاسب ينتقل الفيروس الى الذاكرة ويحدث عدوى لكل قرص يتم تشغيله على الجهاز، ويقوم الفيروس بكتابة نسخة من نفسه على كل قرص سليم ليصيبه بالعدوى[٢٨]. ويسبب هذا النوع من الفيروسات ظهور رسالة خطأ عند تشغيل الحاسب الآلي تتضمن الآتي: ***missing operating system*** أو ***system or hard disk not found***.

وعلى الرغم من أن الانتشار بالنسخ التلقائي يعد أحد السمات المميزة للفيروسات، إلا أن مصطلح فيروس يطلق أيضاً على برامج أخرى مصممة لإلحاق الأذى بالحاسبات على الرغم من أنها لا تستطيع نسخ نفسها، ومنها ما يلي[٢٩]:

١. **أحصنة طروادة** ***Trojan Horses***:

هي برامج تتضمن تعليمات خفية تهدف للتخريب وإلحاق الأذى بالنظام على الرغم من أنه في ظاهره يبدو كأنما يؤدي أعمالاً عادية، فهي توحي للمستخدم بأنها تقوم بعمل معين في حين أنها في واقع الأمر تؤدي عملاً آخر تخريبي في الغالب، فتقوم أحياناً بالتجسس ومتابعة كل ما يتم عمله من إجراءات أو تسجيله من بيانات على الجهاز المصاب بها، وتقوم أحياناً أخرى بإحداث أنواع أخرى من الأذى على الأجهزة المصابة مثل تشفير البيانات أو مسحها أو ما سوى ذلك. ولا تتمكن أحصنة طروادة من نسخ نفسها والالتصاق بالبرامج الأخرى ولكنها تؤدي عملاً معيناً تم تصميمها من أجله.

٢. **القنابل المنطقية** ***Logic Bombs*** **والقنابل الموقوتة** ***Time Bombs***:

هي من أنواع أحصنة طروادة ، وتعمل القنابل المنطقية عند حدوث شرط منطقي محدد مثل بلوغ الموظفين عدداً معيناً أو رفع اسم أحد الموظفين من كشف الرواتب، أو كتابة كلمة معينة، أو عند تشغيل برنامج معين لعدد محدد من المرات. أما القنابل الموقوتة فتعمل وفقاً لتوقيت معين مثل ساعة محددة أو يوم محدد.

٣. **الديدان** ***worms*** :

لا تحتاج الدودة إلى برنامج آخر تلتصق به للقيام بدورها كما هو الحال بالنسبة للفيروس الذي يلزمه حاضن ***host*** لتنفيذ مهمته، ولكنها تعمل بمفردها حيث لديها القدرة على إعادة توليد نفسها والانتقال من ملف الى آخر ومن جهاز إلى آخر متصل بالشبكة لتحقيق الانتشار.
ولا تعمل الديدان على تخريب الملفات وإتلافها كما هو الحال بالنسبة للفيروسات ولكنها تسبب زيادة عبء على تحميل الشبكة حيث تقوم باستهلاك الذاكرة أو المعالج أو الأقراص أو سائر موارد الحاسب، وقد تؤدي بالتالي إلى توقف النظام.

٤. **باب الفخ أو المصيدة** ***Trapdoor***:

يطلق عليها أيضاً الأبواب الخلفية ***backdoors*** ، وتمثل كود يوضع عمداً عند البرمجة لتجاوز نظم الحماية في البرنامج. وهو يسهل على المبرمج الدخول إلى البرنامج والتعديل فيه دون الحاجة إلى اتباع الخطوات التقليدية لذلك.

وعادةً يتم حذف أبواب الفخ بعد الانتهاء من جميع الاختبارات الخاصة بالبرنامج، ولكن في بعض الأحيان تترك تلك الأبواب سواء بقصد أو بدون قصد. وقد يكتشف البعض تلك الأبواب ويستغلها لأغراض تخريبية للتجسس وانتهاك سرية البيانات أو لزرع الفيروسات.

٥. برامج الطوفان *flooders* :

تتمثل في مجموعة كبيرة جداً (مئات أو ألوف) من الرسائل التي تصل من جهات غير معروفة إلى الشبكة عن طريق البريد الإلكتروني أو عن طريق برامج ***ICQ***، وهي بدون شك تسبب إزعاجاً كبيراً حتى وإن كانت لا تسبب ضرراً.

٦. برامج الخداع *spoofing*:

تؤدي إلى تضليل مستقبل المعلومات حيث يبدو أنها مرسلة من جهة معينة في حين أنها في الواقع مرسلة من جهة أخرى؛ الأمر الذي يسمح بدخول المعلومة إلى الشبكة ويجعل مستقبلها يتعامل معها دون معرفة هوية مرسلها الحقيقي.

استخدام البرامج المضادة للفيروسات:

هناك شركات عديدة تنتج برامج مضادة للفيروسات من بينها : ***Symantec,Command,Mcafee*** وغيرها... وتعمل تلك البرامج الآتي:

١) فحص ذاكرة الحاسب عند بدء تشغيله بحثاً عن أي فيروسات.

٢) فحص أقراص التخزين بحثاً عن أي فيروسات، وفي حالة وجودها يتيح إزالتها أو إلغاء الملفات المصابة بها.

٣) فحص الملفات المراد تحميلها على جهاز الحاسب سواء كانت تلك الملفات متاحة من خلال الشبكة أو على أقراص مرنة وذلك للتأكد من سلامتها من الفيروسات.

٤) فحص الملفات سواء المتاحة للمشاركة أم المنقولة عبر الإنترنت أم المرسلة عبر البريد الإلكتروني للتأكد من خلوها من الفيروسات والتنبيه بوجودها إن وجدت وتوفير الحماية ضدها.

٥) الفحص المستمر للنظام للتأكد من خلوه من الفيروسات، والتنبيه عنها في حالة وجودها[٣٠].

سادساً: النسخ الاحتياطي *Backup*:

على الرغم من الاحتياطات الأمنية المتعددة التي قد تتبع لحماية البيانات إلا انه من المحتمل وقوع أي نوع من التلف أو التحريف أو الفقدان للبيانات، لذا كان لابد من تأمين طريقة يمكن من خلالها استعادة البيانات التالفة أو المفقودة أو المحرفة لضمان مستوى أعلى من الحماية للنظام.

ويحقق النسخ الاحتياطي للبيانات هذا المستوى من الحماية، حيث يتم من خلاله إنشاء نسخ احتياطية يتم حفظها سواء في نفس مقر العمل أو خارجه، ويتم تحديثها بصورة منتظمة لضمان أقل قدر من الخسائر في حالة فقدان البيانات الأصلية.

ولابد من تحديد ما ينبغي نسخه احتياطياً ومتى ينبغي نسخه. ويعتمد ذلك على درجة الحماية المطلوب تحقيقها، وعلى كيفية استخدام الشبكة، وكذلك على درجة أهمية البيانات المختزنة على خادم الملفات.

- **البيانات اللازم نسخها:**

لابد من تحديد ما ينبغي نسخه احتياطياً من المعلومات. ويشمل النسخ عادةً كل المعلومات التي لا يمكن إعدادها بسهولة؛ بما في ذلك المعلومات التي ينتجها المستخدم، والمعلومات الأساسية والحيوية الخاصة بالنظام والمختزنة على الخادم، وقواعد البيانات ، والملف الخاص بالمستخدمين، والبريد الإلكتروني.

- **فترات النسخ:**

يتم النسخ على فترات يومية أو أسبوعية أو شهرية وذلك وفقاً لما يلائم العمل؛ فعلى سبيل المثال إذا كانت الشبكة معتمدة كلياً على البيانات المختزنة على خادم الملفات ولا يمكن إنجاز العمل بدونها ؛ ففي هذه الحالة لابد من إجراء عملية النسخ يومياً، وهذا يعني نسخ جميع الملفات الموجودة على خادم الملفات، أما في حالة احتفاظ مستخدمي الشبكة بالبيانات الخاصة بهم على حاسباتهم الشخصية ففي هذه الحالة يمكن عمل نسخة احتياطية كاملة أسبوعياً بدلاً من النسخ اليومي(٣١).

وينبغي أن يجرى النسخ الاحتياطي دورياً على فترات منتظمة محددة مسبقاً وليس بشكل عشوائي؛ فلابد من تحديد يوم معين في كل أسبوع أو ساعة معينة في اليوم وذلك حتى يسهل معرفة الفترة التي ينبغي الرجوع إليها لتصحيح أي خطأ في حالة حدوثه.

وهناك حالات قليلة لا يتم فيها النسخ الدوري بصورة منتظمة وذلك في حالات الملفات شبه الثابتة التي لا يحدث فيها تغيير بصورة مستقلة، الأمر الذي تنتفي معه الحاجة للتحديث المتكرر،

ويكفي أن يتم النسخ على فترات متقاربة في الفترات النشطة التي يحدث فيها تغيير على الملف، في حين تتباعد فترات النسخ في الفترات الميتة التي يقل فيها التغيير(٣٢).

ولابد من متابعة نظام النسخ بصورة دورية للتأكد من فعاليته وسلامته ويتم ذلك عن طريق إجراء عملية استرجاع للمعلومات من النسخ الاحتياطية ومقارنتها بالأصلية، كما ينبغي حفظ سجل مفصل لعمليات النسخ يوفر معلومات مثل تاريخ النسخ ونوعه والشخص الذي قام بإجرائه، وعلى أي وسيط تم النسخ(٣٣).

وهناك أكثر من طريقة تتبع للنسخ الاحتياطي تتمثل في الآتي:

- **النسخ الاحتياطي الكامل *Full Backup*** :

يتم وفقاً له نسخ جميع الملفات المحملة على الخادم بغض النظر عما إذا كان قد أجري تعديل على تلك الملفات من عدمه.

- **النسخ الاحتياطي التراكمي أو التزايدي *Incremental Backup*** :

يتم وفقاً له إجراء نسخ احتياطي للملفات التي تم تعديلها بعد آخر نسخ احتياطي، ويتم في هذه الحالة تعديل سمات الملفات بحيث يظهر أنه أجري لها نسخاً احتياطياً.

- **النسخ الاحتياطي التبايني أو التفاضلي *Differential Backup*** :

يتم وفقاً له إجراء نسخ احتياطي للملفات التي تم تعديلها بعد آخر نسخ احتياطي، ولا تعدل سمات الملفات في هذه الحالة(٣٤).

ويجري النسخ التبايني في كل مرة على البيانات ابتداءً من آخر نسخ احتياطي كامل لها، في حين يجري النسخ التراكمي على البيانات ابتداءً من آخر نسخ احتياطي لها.

وتدعم برامج تشغيل الشبكات عمليات إنشاء النسخ الاحتياطية، والى جانب ذلك فإن هناك برامج أخرى تؤدي ذلك الدور ومنها على سبيل المثال:

Norton Utilities, Fast Back Plus, Central Point Backup.

سابعاً: دعم أجهزة عدم انقطاع التيار *Uninterruptable Power Supply (UPS)* :

يمثل ***UPS*** مولد للطاقة يعمل كمصدر احتياطي في لحظة انقطاع المصدر الاعتيادي للطاقة بحيث يتم بواسطته تشغيل خادم الشبكة ومكوناتها الأخرى لفترة وجيزة تكون كافية لإغلاق

النظام بشكل طبيعي حتى لا يتم فقد البيانات أو تلفها أو تحريفها عند انقطاع التيار الكهربائي.
وبذلك فإن عمل ***UPS*** يتمثل في الآتي:

- الإبقاء على الأجهزة عاملة لفترة وجيزة من الوقت.
- تنفيذ عملية ليتم توقف الأجهزة عن العمل بصورة آمنة دون إحداث تلف أو فقدان للمعلومات (٣٥).

ويتوافر نوعان من أجهزة ***UPS*** وهي على النحو التالي:

أ. مصدر الطاقة الدائمة المباشر ***Online Power Supplies***:

يمثل هذا النوع أجهزة ***UPS*** الحقيقية ويتم وفقاً له تزويد الحاسب بالطاقة بشكل مستمر، حيث يتوافر جهاز ***UPS*** بين مصدر الطاقة الاعتيادية وبين جهاز الحاسب، ويعمل على تزويد الحاسب بالطاقة بصورة مستمرة بغض النظر عما إذا كان هناك انقطاع للطاقة الاعتيادية من عدمه؛ وذلك على اعتبار أن مولد طاقة ***UPS*** يستقبل الطاقة الكهربائية من مصدرها الاعتيادي ويحفظها بداخله ويعمل على تزويد جهاز الحاسب بالطاقة من داخله وليس من مصدرها الرئيسي وبذلك فإن توصيل الطاقة الى الحاسب لن ينقطع في حالة انقطاع المصدر الاعتيادي للطاقة؛ حيث يظل مولد الطاقة ***UPS*** يزود الحاسب بالطاقة الكامنة بداخله لفترة وجيزة جداً تسمح بإغلاقه بطريقة طبيعية.

ب. مصدر الطاقة الدائمة البديل ***Switched Power Supplies***:

يطلق عليه أيضاً ***Standby Power Supplies*** ويعد هذا النوع أقل تكلفة من النوع الأول حيث يتم وفقاً له تفعيل عمل الطاقة الاحتياطية في حالة انقطاع الطاقة الاعتيادية فقط. ويعمل مصدر الطاقة البديل المتصل بالحاسب على مراقبة تقلبات مستوى الطاقة، وفي حالة توقف الطاقة الاعتيادية يقوم بالتحويل إلى مصدر الطاقة البديل ، ويقوم مولد الطاقة في هذه الحالة بتوصيل الطاقة من مصدرها الاعتيادي مباشرة إلى الحاسب، وفي حالة انقطاع الطاقة الاعتيادية تكون هناك فترة توقف بسيطة جداً إلى حين بدء تزويد الحاسب بالطاقة المحفوظة بداخل المولد الاحتياطي(٣٦).

ثامناً: الحماية من خلال الأشخاص:

يقصد بها الأساليب المتبعة لتحقيق الحماية من خلال مستخدمي النظام سواء كانوا موظفين أم مستفيدين:

أ. **الموظفون:**

يعد الموظفون من العناصر الأساسية التي قد تؤدي إلى إلحاق الضرر بالمعلومات وتهديد أمنها سواء بشكل مقصود في حالة رغبتهم الإساءة للهيئة التي يتبعونها لأي دافع من الدوافع (كراهية، أو ملل، أو طمع، أو إثبات الذات) ، أم كانت بشكل غير مقصود بسبب ضعف مستوى إعدادهم فنياً للتعامل مع النظام، لذا ينبغي اتباع ما يلي[٣٧]:

١) تحديد كلمات مرور للموظفين وفقاً لما تم إيضاحه سابقاً، على أن يراعى تحديد صلاحيات كل موظف بما يتناسب مع طبيعة عمله، فمن غير الملائم منح جميع الموظفين صلاحية الدخول إلى جميع مناطق العمل على النظام وإجراء التعديلات على البيانات والبرامج لأن ذلك قد يعرض النظام للخطر، ومن ناحية أخرى فإن منح الصلاحيات بدون حدود أمر لا ضرورة له حيث أن هناك مناطق عمل لا تعني جميع الموظفين ولا تخص عملهم.

٢) اختيار الموظفين بعناية تامة خصوصاً أولئك الذين يتعاملون مع بيانات حساسة والذين يمنحون صلاحيات عالية، حيث ينبغي التأكد من أمانتهم وإخلاصهم وذلك بإجراء تحريات عنهم وملاحظة سلوكياتهم بعد عملهم.

٣) تدريب الموظفين بشكل جيد وذلك تجنباً للعديد من المشكلات التي قد تواجهها الشبكة ومواردها نتيجة لضعف المستوى الفني للعاملين عليها؛ ومنها على سبيل المثال حذف شئ من البيانات بطريقة الخطأ أو تحديث البرامج أو إزالتها بطريقة خاطئة مما يؤثر على النظام والعمل القائم، فلابد من تدريب الموظفين على استخدام الأجهزة بكفاءة من ناحية، وكذلك تدريبهم على سبل التعامل مع المشكلات البسيطة التي قد تواجههم وكيفية التغلب عليها من ناحية أخرى.

٤) التأكد من إزالة بيانات الموظفين المنتهية مدة خدمتهم في المؤسسة من قائمة مستخدمي النظام، وقد يتطلب الأمر تغيير كلمة المرور الخاصة بمجموعة من الموظفين عند انتهاء خدمة أحدهم، وذلك في حالة معرفة الموظف بكلمات المرور الخاصة بالمجموعة.

ويرى البعض ضرورة اتباع إجراءات أخرى حرصاً على الأمن من جانب الموظفين كأن لا تمنح صلاحيات عالية للموظفين حديثي التعيين، وكذلك ضرورة تضمين عقود عمل المتعاقدين لشرط يمنع إفشاء المعلومات الحساسة أو الإجراءات الأمنية للنظام.

ب. **المستفيدون:**

يسري عليهم بعض ما يسري على الموظفين حيث أنه إذا لم يتم تدريب مستخدم النظام بشكل كافي فإنه قد يلحق الضرر بالنظام وذلك بنقل الفيروسات أو إلحاق الضرر بالأجهزة .

وقد يتعمد بعض المستفيدين إلحاق الضرر بالنظام في حالة تصورهم أن هناك إجـــراءات أمنيـــة متشددة تتبع ضدهم بشكل يؤدي إلى إزعاجهم بدون مبرر مقنع بالنسبة لهم، مما يضـــطرهم إلى التحايل على النظام ومحاولة إلحاق الضرر به، ومن هنا يرى البعض ضرورة توعيـــة المســـتفيدين بالأسباب التي تدعو إلى استخدام كلمات المرور، والخروج من النظام ***log off*** بطريقة سليمة ، وتعريفهم بالأسباب التي تدعو إلى ضرورة عمل مسح للأقراص المرنة في حالة جلبـــها معهـــم للتأكد من خلوها من الفيروسات[٣٨].

شبكة المكتبات بجامعة أم القرى:

تم إنشاء شبكة المعلومات في عمادة شئون المكتبات في أواخر عام ١٤١٧هـــ، ويعـــد إنشـــاؤها جزء من تنفيذ المرحلة الثانية من مشروع توسعة الشبكة المحلية للجامعة والتي شملت إلى جانب عمادة شئون المكتبات كل من معهد خادم الحرمين الشريفين، ومعهد البحوث العلميـــة وإحيـــاء التـــراث الإسلامي، ومركز الوسائل وتقنيات التعليم، وعمادة الدراسات الجامعية.

وبدأت شبكة المكتبات في المرحلة الأولى لإنشائها لتربط بين الحاسبات بداخل مقر المكتبة المركزيـــة للطلاب بمنطقة العزيزية بمكة المكرمة، ثم توسعت في عام ١٤٢١هـــ لتضم المكتبة المركزية للطالبات بمكة المكرمة، وسيتم بإذن الله تعالى لاحقاً التوسع في الشبكة لتربط كل من مقر الجامعـــة بمنطقـــة العابدية وكذلك المكتبة المركزية للطلاب في فرع الجامعة بمدينة الطائف.

وتوفر الشبكة للمكتبات المشاركة في الآتي:

- برنامج الأفق الذي يمثل النظام المتكامل الذي تعمل به المكتبات التابعة للعمادة.
- قواعد البيانات التي تشترك فيها العمادة على أقراص مدمجة.

هذا الى جانب ما تتيحه شبكة الجامعة من الاتصال بشبكة الإنترنت حيـــث تم توصـــيل مركـــز المعلومات والحاسب الآلي في الجامعة بشبكة الإنترنت عن طريق مدينة الملك عبد العزيز للعلـــوم والتقنية وعن طريق شركة الاتصالات السعودية.

وتخصص عمادة شئون المكتبات خادم رئيسي واحد للشبكة بداخلها حيـــث يـــتم تشـــغيل البرنامج الآلي المتكامل للمكتبات عليه وهو نظام الأفق ***Horizon***، وكـــذلك يـــتم تحميـــل الأقراص المدمجة التي تشترك فيها العمادة وتطبيقاتها بحيث تعمل على الخادم نفسه، كما تخصـــص العمادة خادم احتياطي للشبكة كأحد أنظمة احتمال الخطأ ***fault tolerance*** التي توفرها لضمان استمرار عمل الشبكة في حالة توقف الخادم الرئيسي. ويتواجد الخادم الاحتياطي في مقر مركز المعلومات والحاسب الآلي ، أي خارج مقر عمادة شئون المكتبات.

وقد أجرت الباحثة دراسة حالة على شبكة مكتبات جامعة أم القرى، ووجدت أن الحفاظ على أمن المعلومات في الشبكة يعد مسئولية موزعة ما بين عمادة شئون المكتبات وبين مركز المعلومات والحاسب الآلي والتطوير الجامعي، وقد وضع مركز المعلومات قواعد تنظيمية لضبط العمل على الحاسبات واستخدام الشبكات بشكل يراعى فيه العديد من الجوانب ومن بينها حماية أمن المعلومات على الشبكات وتم اعتماد تلك القواعد من قبل إدارة الجامعة حتى يتم العمل بموجبها في مختلف الإدارات والأقسام والعمادات ومن بينها عمادة شئون المكتبات (وسيشار إلى تلك القواعد في الدراسة لاحقاً بالقواعد الصادرة عن إدارة الجامعة). وفيما يلي توضح الباحثة الأساليب المتبعة لحماية أمن المعلومات في شبكة مكتبات الجامعة:

أولاً: الحماية الفيزيائية (المادية):

تتبع العمادة عدداً من العناصر التي تكفل بعض جوانب الحماية الفيزيائية للشبكات ومواردها ومن ذلك ما يلي:

١) تخصص مكاناً مستقلاً لحفظ أجهزة الخادم بداخل مبنى المكتبة المركزية للطلاب.

٢) استخدام كابلات الألياف الضوئية ***fiber optics*** للتمديدات الداخلية، ويضمن هذا النوع من الكابلات درجة كبيرة من الحفاظ على أمن المعلومات أثناء نقلها عبرها.

٣) الحرص على تركيب الكابلات بشكل يضمن حمايتها؛ فلا توضع فوقها قطع الأثاث أو ما شابه ذلك.

٤) توفر عوازل بلاستيكية لتغطية كابلات الشبكة بهدف تحقيق أكبر قدر من الحماية لها.

ويلاحظ أن هناك جوانب عديدة للحماية المادية لم تحرص عليها العمادة ومن ذلك توفير المراقبة للمكان سواء عن طريق أشخاص أم كاميرات مراقبة، وكذلك استخدام أجهزة إنذار للتنبيه في حالة دخول شخص غير مصرح له إلى موقع الخادم. وتعتقد الباحثة أنه من غير الضروري في المكتبات توفير هذه الدرجة من الحماية وذلك على اعتبار أن مستوى الحماية المطلوب يختلف وفقاً لاختلاف درجة حساسية المعلومات وسريتها ومن غير المتوقع أن يتسلل أحد الأشخاص إلى موقع الخادم لسرقة قواعد بيانات المكتبة أو ليتعمد إلحاق تلفيات بها على سبيل المثال، وإن كان تصرف كهذا وارد في جهات أخرى مثل أجهزة المخابرات في الدولة أو الجهات التي تحتفظ بمعلومات سرية عن منتجات معينة، أو ما شابه ذلك.

وقد تضمنت القواعد التنظيمية الصادرة عن إدارة الجامعة بعض القواعد التي من شأنها أن تكفل بعض الجوانب الأخرى المتعلقة بحماية أمن الشبكة ومواردها من الناحية الفيزيائية؛ فعلى سبيل المثال نصت تلك القواعد على الآتي:

١. منع تغيير إعدادات وتوصيلات الشبكات من قبل المستخدمين سواء كان ذلك فعلياً أم منطقياً.

٢. منع تركيب عتاد أو برامج دون التنسيق مع مدير النظام (مثل تركيب جهاز مودم على الحاسب الشخصي أو وسيط إنترنت ***proxy***) .

٣. منع التنصت أو مراقبة الاتصالات الإلكترونية الخاصة بمستخدمين آخرين.

ثانياً: ضبط الوصول للشبكة ومواردها:

تحدد العمادة حسابات لمستخدمي الشبكة ***accounts*** تتضمن أسماء تعريف وكلمات مرور، وتحدد ذلك حسب المواقع في بعض الحالات وحسب المستخدمين في حالات أخرى.

إتاحة الوصول حسب الموقع:

تتيح العمادة الوصول للفهرس العام للجمهور ***PAC*** باستخدام اسم تعريف وكلمة مرور للموقع نفسه وتحدد صلاحيات المستخدم بحيث يتاح له البحث والقراءة من قاعدة البيانات فقط ولا يتاح له الدخول إلى قاعدة بيانات الفهرسة أو غيرها أو التعديل في البيانات، وتتيح العمادة الوصول حسب الموقع أيضاً لقواعد البيانات الإلكترونية التي تشترك فيها العمادة على أقراص مدمجة، وكذلك قواعد البيانات الإلكترونية التي تشترك فيها من خلال شبكة الإنترنت حيث تتيح الوصول إليها باستخدام اسم تعريف وكلمة مرور لكل قاعدة من تلك القواعد على أساس الموقع.

وتجدر الإشارة إلى أن المكتبة لا تحدد استخدام قواعد البيانات الخاصة بها من عنوان معين ***IP address*** وهو العنوان الخاص بجامعة أم القرى، ولكن يمكن الدخول إلى قواعد البيانات (حتى وقت إجراء هذه الدراسة) من أي عنوان عبر شبكة الإنترنت. ومن ناحية أخرى تخصص العمادة أيضاً أسماء تعريف وكلمات مرور حسب الموقع للعمل في قسم الإعارة بالمكتبة. وقد أوضح سعادة مدير المكتبة أن تحديد الإتاحة بقسم الإعارة كان يتم في السابق وفقاً للأشخاص وقد تم تغيير ذلك النظام لظروف وقتية معينة؛ وبذلك فإن هذا الوضع يعتبر مؤقت حيث سيجري قريباً تعديل النظام لتصبح الإتاحة حسب الأشخاص.

إتاحة الوصول حسب الأشخاص:

يتم ذلك في قسم الإجراءات الفنية بمكتبة الطلاب وكذلك مكتبة الطالبات؛ حيث يتاح الدخول إلى الموقع الخاص بالفهرسة والإضافة إلى قواعد البيانات والحذف منها والتعديل فيها باستخدام اسم تعريف وكلمة مرور خاصة بكل موظف وموظفة من الموظفين والموظفات على حده.
وقد تبين للباحثة عدم اختلاف الصلاحيات الممنوحة لكل موظف أو موظفة بقسم الإجراءات الفنية؛ بل إن لرئيس القسم نفس الصلاحيات دون أي اختلاف عن موظفي القسم.

ولعل اعتماد العمادة على تحديد أسماء التعريف وكلمات المرور للمواقع نفسها يحقق السهولة في الاستخدام للمستفيدين، كما أنه يحقق أكبر فائدة من قواعد البيانات المستخدمة. وقد لا يكون لدى العمادة الدافع الذي يجعلها تخصص كلمات مرور للأشخاص فيما يتعلق بقواعد البيانات التي تشترك فيها سواء على أقراص مدمجة أم من خلال شبكة الإنترنت؛ خصوصاً إذا لم يكن هناك تعارض بين هذا الإجراء وبين شروط تراخيص استخدام تلك القواعد التي تحفظ حقوق الملكية الفكرية للناشرين. فمن جانب العمادة ليس هناك معلومات سرية في تلك القواعد ترغب في حفظها بعيداً عن المستخدمين، بل أنها تسعى إلى تحقيق أكبر قدر من الاستفادة من تلك القواعد سواء من داخل المكتبة أم من خارجها، لمنسوبي المكتبة أم غيرهم لأن في ذلك ما يحقق الجدوى من اشتراك العمادة في تلك القواعد، يضاف إلى ذلك أن الصلاحيات التي يمنحها موردو تلك القواعد للمستخدمين تقتصر على الاستخدام ولا تتيح التعديل أو التغيير في البيانات المختزنة في تلك القواعد.

أما فيما يتعلق بمواقع العمل المكتبي كالإعارة فإن استخدام كلمة مرور للموقع تعد طريقة غير آمنة بالدرجة الكافية؛ وذلك على اعتبار أن حرص الشخص على حفظ كلمة المرور الخاصة بالموقع لا ترقى في درجتها إلى حرصه على حفظ كلمة المرور الخاصة به؛ وبالتالي فإن الأمر يتطلب تخصيص كلمات مرور لكل مستخدم على حده؛ بل إنه يتطلب تحديد صلاحيات كل موظف بما يتلاءم مع حجم عمله؛ فهناك نشاطات في قسم الإعارة وكذلك في قسم الفهرسة ينبغي ألاّ تترك حرية ممارستها لجميع الموظفين؛ ومن ذلك على سبيل المثال النشاطات المتعلقة بضبط غرامات الإعارة وصلاحيات رفعها عن المستفيدين وكذلك التعديل والتغيير في قواعد بيانات الفهرسة التي تم حفظها، وينبغي لتحقيق مستوى أعلى من أمن المعلومات أن يتم تحديد ممارسة تلك الصلاحيات وما شابهها بحيث تكون متاحة لرئيس القسم فقط.

وينبغي الإشارة إلى لرئيس قسم الحاسب الآلي في العمادة ونائبه الحق في تعديل صلاحيات مستخدمي شبكة معلومات المكتبة المحفوظة في ملفات المستخدمين الخاصة بنظام الأفق، ويتم التعديل عادة وفقاً لمقتضيات العمل والحاجة لإجراء التعديل.

وعلى الرغم من ضبط العمادة لعمليات الوصول الى الشبكة ومواردها باستخدام أسماء تعريف وكلمات مرور لمستخدميها إلا أنها لا تراعي اختيار كلمات صعبة الكشف من قبل الآخرين؛ فلا تحرص على سبيل المثال أن تجعل كلمات المرور طويلة، أو أن تخلط فيها بين الحروف والأرقام أو الرموز، ولكنها على العكس من ذلك تحرص على اختيار كلمات مرور قصيرة وسهلة التذكر، كما أنها لا تحرص على تغيير كلمات المرور على فترات منتظمة، ولكن يتم تغيير كلمات المرور وفقاً لتغيير المهام المطلوبة للمستخدم.

ولا تقوم العمادة بمراقبة ***Monitoring*** لمستخدمي الشبكة الخاصة بها ؛ وبالتالي فإنها لا تعمل على متابعة مرات دخول المستخدمين وخروجهم، ولا تتابع كذلك ما يقومون بعمله على الشبكة وما يدخلون عليه من مواقع أو ما سوى ذلك.

وإذا كان ما سبق يوضح الضوابط والإجراءات التي تتبعها العمادة لضبط إتاحة الوصول إلى شبكة المعلومات الخاصة بها ، فإن هناك ضوابط محددة في القواعد التنظيمية الصادرة عن إدارة الجامعة حيث تؤكد تلك القواعد على ضرورة الالتزام باستخدام الأجهزة والخدمات والشبكات المصرح بها فقط من قبل إدارة الجامعة، وتشير إلى أن الحصول على تصريح لاستخدام جزء من الشبكة لا يعني السماح باستخدامها كلها. كما تنص على ضرورة المحافظة على كلمة المرور الخاصة بكل شخص وضمان عدم إطلاع الآخرين عليها واتباع التعليمات الخاصة بها.

وقد حددت تلك القواعد صلاحيات مستخدمي شبكة الجامعة والأوقات المصرح بالاستخدام فيها من أي موقع بالجامعة بما في ذلك المكتبات وذلك بتقسيمهم الى ثلاث فئات وفقاً لصلاحياتهم، وتأتي الفئات على النحو التالي:

١. الفئة الأولى: تشمل جميع أعضاء الهيئة الأكاديمية وطلاب الدراسات العليا وموظفي الجامعة ممن يتطلب عملهم استخدام شبكة الإنترنت، ويصرح لهم باستخدام البريد الإلكتروني، والشبكة الداخلية للجامعة ***intranet***، والشبكة العنكبوتية العالمية ***world wide web*** طوال اليوم.
٢. الفئة الثانية: وتشمل جميع موظفي الجامعة، ويصرح لهم باستخدام البريد الإلكتروني والشبكة الداخلية للجامعة ***intranet*** طوال اليوم؛ في حين تحدد ساعات استخدامهم للويب في الفترات ما بين ٧-٩ صباحاً و ٢-٤ مساءً.
٣. الفئة الثالثة: وتشمل طلاب وطالبات الجامعة، ويصرح لهم باستخدام الشبكة من خلال معامل الحاسب الآلي في الجامعة، وحسب الأوقات المحددة لذلك.

وترى الباحثة أن هذا التقسيم ملائم جداً ؛ حيث يتم من خلاله تلافي بعض السلبيات التي قد تحدث عند فتح المجال لاستخدام شبكة الإنترنت للجميع طوال فترة الدوام الرسمي؛ الأمر الذي قد يؤثر على أداء الموظفين لأعمالهم، ومن ناحية أخرى فإن هذا النظام يتعامل مع الموظفين الذين يتطلب عملهم استخدام الشبكة بشكل يحفظ لهم حقهم في أداء عملهم، وبذلك يتم توزيع الصلاحيات حسب حاجة العمل والقائمين عليه.

ثالثاً: برامج الحماية ضد الفيروسات:

تستخدم عمادة شئون المكتبات برنامج وقاية ضد الفيروسات على أجهزة الخادم الخاصة بها وكذلك على محطات العمل الموجودة في كل من المكتبة المركزية للطلاب والمكتبة المركزية للطالبات. وتستخدم العمادة برنامج ***Norton AntiVirus (NAV)*** الذي تصدره شركة ***Symantec corporation*** ويتميز البرنامج بالآتي[٣٩]:

١. يقدم برنامج ***NAV*** حماية من الفيروسات المعروفة التي تم تحليلها من قبل باحثي الفيروسات، وكذلك الفيروسات الجديدة وغير المعروفة.

٢. يوفر البرنامج نظام إنذار مركزي يعمل في حالة اكتشاف فيروس على النظام.

٣. يوفر البرنامج تحديثاً مجانياً له عبر الإنترنت باستخدام تقنية ***Live updates*** المزود بها البرنامج.

٤. يوفر مركز أبحاث ***Symantec*** دعماً فنياً لمقتني البرنامج.

٥. يعد البرنامج سهل الاستخدام والتحديث.

وفي دراسة أجريت حول البرامج المضادة للفيروسات ونشرت في مجلة ***PC Magazine*** تم اختبار ست حزم برمجية مضادة للفيروسات تعمل في بيئة ويندوز، وقد توصلت الدراسة إلى أن ***NAV*** من أفضل تلك البرامج بل إنه تم اختياره كبديل أمثل من قبل المحررين حيث وجد أن أدائه مطابق لما تعلن عنه الشركة ، ففي العينة التي تم تطبيق الدراسة عليها تبين أن ***NAV*** قد تمكن من اكتشاف جميع الفيروسات الموجودة على لائحة الفيروسات الفعلية ***wild list*** المحددة من قبل جمعية ***NCSA*** كما أن أدائه كان حسن في التغلب على الفيروسات الماكروية ، إضافة إلى اكتشافه نسبة كبيرة جداً ٩٩.٣% من الفيروسات النظرية ***Zoo*** التي اكتشفت في المختبرات و لم تسجل أي إصابات بها في الواقع. ويعاب على البرنامج بطئ أدائه مقارنة بغيره من البرامج المضادة للفيروسات[٤٠].

وعلى الرغم من المميزات العديدة لبرنامج *NAV* وإمكانياته العالية إلاّ أن العمادة لا تستفيد من معظم المميزات بل إنها لا تعمل على تحديث البرنامج على جهاز الخادم أو على محطات العمل؛ الأمر الذي عرض بعض محطات العمل في المكتبة المركزية للطلاب، وكذلك بعض محطات العمل في المكتبة المركزية للطالبات إلى الإصابة بالفيروسات أكثر من مرة، وقد تمت معالجة الأمر دون أن يلحق الضرر بالشبكة ومواردها وذلك بإحالة الأجهزة المصابة إلى مركز المعلومات والحاسب الآلي والتطوير الجامعي لحل المشكلة وإجراء الصيانة اللازمة للأجهزة. ولاشك أن عدم تحديث برنامج الحماية ضد الفيروسات يجعل البرنامج لا قيمة له وذلك على اعتبار أنه لن يستطيع مقاومة عشرات الفيروسات التي تظهر يومياً في العالم.

وتراعي إدارة الجامعة توجيه العديد من الإرشادات لمستخدمي الشبكات للتقليل من مخاطر التعرض للفيروسات، وقد تم تحديد تلك الإرشادات في شكل نصائح أمنية اشتملت عليها قواعد التعامل مع الأنظمة الحاسوبية والشبكات والصادرة عن إدارة الجامعة؛ حيث تضمنت تلك النصائح الإرشادات التي تكفل الحماية من الفيروسات ومن بينها ما يلي:

١. المحافظة على الجهاز من الفيروسات بتركيب برامج مكافحة الفيروسات وتحديثها بشكل دوري.
٢. الحذر من الملفات المرفقة مع الرسائل الإلكترونية والتأكد من خلوها من الفيروسات أو البرامج التي تمكن الآخرين من اختراق النظام.
٣. عدم تحميل برامج من مواقع غير معروفة أو غير موثوق بها من خلال شبكة الإنترنت.

رابعاً: النسخ الاحتياطي:

تقوم العمادة بعمل نسخ احتياطية لقواعد بياناتها وذلك تحسباً لوقوع أي طارئ يحدث تلف لتلك البيانات.. ولا تحرص العمادة على عمل نسخ احتياطية من الملف الخاص بالمستخدمين والمتضمن كلمات المرور الخاصة بهم وحقوقهم، كما لا تحرص على عمل نسخ احتياطية من مراسلاتها البريدية. وبذلك تكون عمادة شئون المكتبات قد خصصت عمليات النسخ الاحتياطي لقواعد البيانات الببليوجرافية التي تمثل مقتنيات المكتبة من مصادر المعلومات، وكذلك سجلات الإعارة.

ويتم النسخ بصورة منتظمة بحيث يتم إجراء نسخاً احتياطياً تراكمياً ***incremental backup*** مرة كل أسبوع على القرص الصلب في حين يتم إجراء نسخاً احتياطياً كاملاً ***full backup*** مرة كل شهر على أقراص مدمجة. وبذلك فإنه في حالة تعرض البيانات للتلف أو الفقدان لا قدر الله فإن العمادة ستستعين بآخر نسخة احتياطية كاملة بالإضافة إلى جميع النسخ الاحتياطية التراكمية التي تمت منذ آخر نسخ احتياطي كامل؛ وذلك على اعتبار أن النسخ الاحتياطي التراكمي يجرى على البيانات منذ آخر نسخ احتياطي لها وليس كحال النسخ التبايني ***differential backup*** الذي يجري فيه النسخ الاحتياطي على المعلومات منذ آخر نسخ احتياطي كامل لها؛ وبالتالي ففي حالة فقدان البيانات يكتفى بالرجوع لآخر نسخة للنسخ الاحتياطي التبايني إلى جانب آخر نسخة احتياطية كاملة.

وتعد الفترة التي تخصصها العمادة للنسخ الاحتياطي متباعدة إلى حد ما ، وقد يكون من الملائم أن يتم إعداد النسخ التراكمي على فترات أكثر تقارباً؛ وذلك على اعتبار أن إضافة المعلومات إلى قاعدة البيانات يتم بصورة يومية من كل من مكتبة الطلاب ومكتبة الطالبات حيث تجري الفهرسة تعاونياً في العمادة. ويتم يومياً إدخال بيانات فهرسة تصل في المتوسط إلى (٧٩) تسجيلة فهرسة—وذلك وفقاً لما أشار إليه نائب رئيس قسم الحاسب الآلي في العمادة من خلال البيانات الموضحة في التقارير اليومية للأسبوع الثاني من شهر مايو لعام ٢٠٠١م– وبالتالي فإن الإبقاء على قاعدة البيانات دون إجراء نسخاً احتياطياً لها لمدة أسبوع يجعل بيانات حوالي (٣٩٥) تسجيلة فهرسة في المتوسط معرضة للفقدان خلال تلك الفترة —والمتمثلة في خمسة أيام بعد استبعاد يومي الإجازة الأسبوعية — هذا إلى جانب سجلات الإعارة المعرضة للفقدان خلال الفترة نفسها .

وقد تتحاشى العمادة السلبيات التي قد تقع بسبب تباعد الفترة وطولها ما بين كل نسخ احتياطي والتالي له عن طريق توجيه الموظفين إلى ضرورة عمل نسخ احتياطية للبيانات التي تخصهم بصفة يومية وذلك تمشياً مع ما نصت عليه قواعد التعامل مع الأنظمة الحاسوبية والشبكات الصادرة عن إدارة الجامعة والتي نصت على أن مستخدم النظام مسئول عن حفظ نسخة احتياطية من البيانات التي تخصه، وضرورة متابعة ذلك بشكل دوري. وبتتبع الباحثة لمدى تطبيق ذلك فعلياً في مكتبات الجامعة وجدت أن موظفات قسم الإجراءات الفنية بالمكتبة المركزية للطالبات لا يقومون بعمل نسخاً احتياطية للبيانات المدخلة يومياً من قبلهم وكذلك الحال بالنسبة للموظفين في المكتبة المركزية للطلاب سواء العاملين منهم بقسم الإجراءات الفنية أم في قسم الإعارة.

وتقوم العمادة بعمل نسخة احتياطية واحدة ، يتم حفظها على قرص مدمج CD وذلك لسعة هذا الوسيط التخزينية العالية التي تتناسب مع ضخامة حجم البيانات، ويتم تسجيل تاريخ النسخ على القرص ، وتحفظ النسخة في مركز المعلومات والحاسب الآلي والتطوير الجامعي حيث يتم إعدادها عن طريق نفس المركز وذلك من خلال جهاز الخادم الاحتياطي المتوافر لديهم؛ وبذلك فإن العمادة تحرص على تأمين النسخة الاحتياطية خارج مقر العمادة بعيداً عن النسخة الأصلية، ولا شك أن في ذلك الإجراء تأمين للنسخة الاحتياطية من أن يلحقها التلف في حالة تعرض الموقع نفسه لأي طارئ.

خامساً: الحماية من خلال الأشخاص:

لم يتم تدريب الموظفين بعمادة شئون المكتبات على مواجهة المشكلات التي قد تعترضهم أثناء استخدامهم للحاسبات ونظم الشبكات؛ وذلك على اعتبار أن هناك متخصصين يقومون بمهمة صيانة الحاسبات في الجامعة نفسها؛ وبذلك فإن العمادة تعمل على إرسال الأجهزة الى جهة الاختصاص في الجامعة عند تعرضها لأي نوع من المشكلات، أو يتم استدعاء أحد المتخصصين إلى المكتبة لحل المشكلة.

وتعتقد الباحثة أنه من الملائم تدريب الموظفين أو بعضهم على بعض الأساسيات التي تؤهلهم للتعامل مع المشكلات البسيطة لتلافي تعطل العمل في حالة وجود مشكلات بسيطة لا تتطلب فنيين متخصصين في صيانة الشبكات أو الحاسبات.

ومن إيجابيات الوضع الحالي أن العمادة تتجنب المخاطرة بقيام البعض بمحاولات للإصلاح قد تؤدي إلى إحداث مشكلات أكبر مثل تلف المعلومات أو موارد الشبكة وتجهيزاتها، وذلك نظراً لعدم تدريب الموظفين على معالجة المشكلات، وبذلك فإنها تحيل الأمر إلى جهة الاختصاص.

ولتجنب سوء استخدام المستفيدين من خدمات المكتبات للشبكة فإن استرجاع المعلومات من خلال شبكة الإنترنت أو الانترانت يتم في المكتبة المركزية للطلاب عن طريق الموظف المختص بعد تعبئة المستفيد لنموذج مخصص لذلك.

أما في المكتبة المركزية للطالبات فيتاح استخدام النظام للمستفيدات سواء عن طريق الموظفة المختصة أم عن طريق المستفيدة نفسها؛ إلا أن المكتبة تتبع بعض الخطوات لحماية أمن الشبكة ومواردها ومن ذلك:

أ. مراقبة المكان من قبل الموظفة المختصة لملاحظة سوء استخدام الأجهزة وموارد الشبكة من قبل بعض المستفيدات.

ب. تقديم خدمات تدريب على استخدام النظام للمستفيدات وذلك لتجنب الاستخدام الخاطئ من قبل البعض.

ج. منع استخدام المستفيدات للأقراص المرنة إلا بعد عرضها على الموظفة المختصة للتأكد من خلوها من الفيروسات.

د. توعية المستفيدات وإرشادهن حول استخدام الخدمات الإلكترونية، وتحرص المكتبة على سبيل المثال على أن توضح للمستفيدات السبب الذي يدعو الى ضرورة عرض الأقراص المرنة على الموظفة، وتعلن المكتبة ضوابط استخدم الخدمات الإلكترونية في لوحة إرشادية في موقع تقديم الخدمة.

وتجدر الإشارة إلى أن العناصر السابقة قد وردت في القواعد التنظيمية الخاصة بتقديم الخدمات الإلكترونية في المكتبة المركزية للطالبات والتي وضعتها كاتبة هذه الدراسة في تاريخ ١٤٢١/٧/٢٤هـ، وتمت الموافقة على تطبيقها من قبل سعادة عميد شئون المكتبات. وقد تضمنت تلك القواعد كل من الجوانب الخاصة بالاستخدامات المشروعة للنظام، ومدة الاستخدام المتاحة لكل مستفيدة، وضوابط خدمات التدريب والإرشاد المرتبطة بالخدمات الإلكترونية، وكذلك ضوابط خدمات الطباعة والنسخ على أقراص مرنة. وقد تمت مراعاة بعض الجوانب التي تضمن حماية أمن الشبكة ومواردها من الناحية المتعلقة بالمستخدمين.

و لم تغفل القواعد التنظيمية الصادرة عن إدارة الجامعة الاهتمام بالجانب الخاص بالمستخدمين، وقد تناولت العديد من الجوانب الهامة ومن بينها على سبيل المثال:

١. توجيه النصح للمستفيدين بما يكفل توعيتهم ببعض الجوانب الأساسية التي من شأنها الحد من المخاطر التي قد تهدد أمن المعلومات وسلامتها؛ بما في ذلك الفيروسات أو الاختراق، وكذلك تضمن تقليص حجم الخسائر في حالة حدوثها من خلال توجيه المستخدمين الى ضرورة الاهتمام بالنسخ الاحتياطي للبيانات. وقد سبقت الإشارة إلى أبرز تلك النصائح المتعلقة بالحماية ضد الفيروسات في موقع آخر من هذه الدراسة.

٢. تحديد المسئوليات التي تقع على عاتق مستخدم النظام والتي من شأنها حماية أمن المعلومات والشبكات ومن ذلك:

أ. ضرورة تقيد المستخدم بالتعليمات الصادرة بشأن حفظ الأمن الإلكتروني.

ب. ضرورة التزامه بأنظمة الاستخدام الخاصة بالشبكات.

ج. مسئولية المستخدم عن استخدامه، وعدم جواز إساءة الاستخدام حتى في حالة وجود ثغرات أمنية في النظام.

د. ضرورة إبلاغ مسئولي النظام والشبكات في الجامعة عن أي إخلال بالأمن الإلكتروني.

ه. مسئولية المستخدم عن حماية البيانات السرية والحساسة المسئول عنها.

٣. تحديد الاستخدامات الممنوعة التي من شأنها إلحاق الضرر بالشبكة وأمن المعلومات ومن ذلك:

أ. استخدام النظام للدخول على حسابات الآخرين ***accounts***، سواء تم ذلك بمعرفة صاحب الحساب أم دون معرفته.

ب. تعمد استخدام الخدمة واستغلالها بطريقة تعرض الشبكة الداخلية للخطر أو تؤدي إلى فتح ثغرات أمنية في الشبكة.

ج. الاستخدام الذي يمكن أن يؤدي إلى تهديد أو تخريب أو إزعاج أو مضايقة لأي شخص أو جهة أو أمنها الإلكتروني: مثل إرسال بريد إلكتروني بشكل متكرر وغير مرغوب فيه، أو لغرض الغش ، أو لخداع الآخرين.

د. محاولة فك تشفير بيانات الآخرين في الأنظمة الحاسوبية.

ه. العبث أو الاطلاع على معلومات خاصة بمستخدمين آخرين.

و. نشر الفيروسات.

ز. استخدام الأنظمة الحاسوبية للجامعة للدخول غير المشروع لأنظمة حاسبات أو شبكات أو مصادر معلومات دون الحصول على إذن.

ح. انتحال شخصية شخص أو جهاز آخر.

ط. إشراك الآخرين في الحسابات الشخصية أو التنازل لهم عن الحسابات.

ويلاحظ أن إدارة الجامعة اهتمت بالجوانب المتعلقة بالمستخدمين إدراكاً منها لدورهم الكبير في الحفاظ على أمن المعلومات، كما يلاحظ أن الجامعة لم تكتف بوضع قواعد لكفالة أمن الشبكة الخاصة بها فقط، وإنما وضعت قواعد أخرى تمنع أي تعدي على أمن الشبكات الأخرى؛ الأمر الذي يحتسب لتلك القواعد من وجهة نظر الباحثة وذلك من جانبين:

أ. أن في ذلك مراعاة لما تقتضيه أخلاقيات تبادل المعلومات والاستفادة من مصادرها.

ب. أن في ذلك حماية لشبكة الجامعة نفسها حيث أن تعرض الآخرين للأذى من خلال شبكة الجامعة قد يؤدي في المقابل الى ردة فعل من الآخرين قد تلحق الأذى بشبكة الجامعة ومواردها.

أساليب الحماية غير المستخدمة في الشبكة:

على الرغم من استخدام العمادة لأساليب متعددة للحماية إلاّ أن هناك أساليب أمنية أخرى لم تستخدمها العمادة ومن ذلك ما يلي:

١) الحوائط النارية *firewalls*

لا تدعم العمادة شبكة المعلومات الخاصة بها بأي من أنواع الحوائط النارية، وقد أوضح المسئول عن الشبكات في مركز المعلومات والحاسب الآلي بأن شبكة الجامعة مزودة بحائط ناري يتمثل في برنامج محمل على خادم شبكة الجامعة، كما أوضح بأن الوصول إلى الشبكة الداخلية للمكتبة وقواعد بياناتها لا يمكن أن يتم إلا من خلال موقع الجامعة وبالتالي فإن ذلك الحائط من وجهة نظره كافٍ لتأمين الشبكة المحلية للعمادة. وترى الباحثة أن توفير حائط ناري للشبكة الداخلية للمكتبات من شأنه أن يوفر لقواعد بياناتها الحماية من أي اقتحام من خارج حدود العمادة بما في ذلك الجهات الأخرى بالجامعة وهو ما لا يمكن تحقيقه من خلال الحائط الناري لشبكة الجامعة الذي من شأنه أن يوفر الحماية من الجهات الخارجية.

٢) دعم أجهزة عدم انقطاع التيار الكهربائي *UPS*

تعرضت شبكة العمادة لبعض المشكلات بسبب الانقطاع المفاجئ للتيار الكهربائي منذ شهور مضت، وعلى الرغم من ذلك فإن العمادة لم توفر أجهزة ***UPS*** حتى تاريخ إعداد هذه الدراسة؛ الأمر الذي يجعل موارد الشبكة عرضة للتلف أو الفقدان نتيجة لعدم إغلاق الملفات بصورة صحيحة عند التعرض للانقطاع المفاجئ في التيار الكهربائي.

٣) التشفير *Encryption*

تتبادل العمادة الرسائل مع جهات متعددة عبر الإنترنت باستخدام البريد الإلكتروني ولا تستخدم في ذلك أساليب تشفير البيانات عند نقلها عبر الشبكة. وقد يرجع السبب في ذلك إلى عدم نقل بيانات سرية عبرها.

النتائج والتوصيات:

توصلت الدراسة إلى النتائج التالية:

١. تهتم عمادة شئون المكتبات بجامعة أم القرى بتطبيق أساليب متعددة لحماية أمن المعلومات على الشبكة الخاص بها ، وتتمثل تلك الأساليب في الآتي:

أ. تأمين الشبكة من الناحية المادية باتباع إجراءات عديدة خاصة بالمكان والتمديدات.

ب. ضبط إتاحة الوصول إلى شبكة المكتبات وذلك بتخصيص حسابات ***accounts*** للموقع أحياناً وللأشخاص في أحيان أخرى.

ج. عمل نسخة احتياطية واحدة كاملة على قرص مدمج مرة كل شهر، إضافة إلى عمل نسخ احتياطي تراكمي على القرص الصلب مرة كل أسبوع.

د. استخدام برنامج ***Norton AntiVirus*** للحماية من الفيروسات على كل من خادم الشبكة ومحطات العمل.

ه. تحقيق الحماية من الاستخدام السيئ للمستفيدين من خدمات المكتبة من خلال بعض الإجراءات المتمثلة في تقييد الاستخدام بحيث يكون عن طريق الموظف المختص بالمكتبة المركزية للطلاب، وعن طريق بعض الإجراءات التنظيمية لاستخدام الشبكة ومواردها في المكتبة المركزية للطالبات.

و. اعتماد إدارة الجامعة لبعض القواعد التنظيمية لاستخدام الشبكات في الجامعة والتي قام بوضعها مركز المعلومات والحاسب الآلي والتطوير الجامعي، وتضمن تلك القواعد تحقيق جانب كبير من الحماية الأمنية لشبكات الجامعة ككل والتي تعد شبكة المكتبات واحدة منها.

٢. تفتقد العمادة تطبيق بعض الأساليب الأمنية الضرورية مثل الحوائط النارية، ودعم أجهزة عدم انقطاع التيار الكهربائي، ونظام التشفير وذلك على الرغم من أهميتها.

٣. يوجد بعض الجوانب السلبية في تطبيق بعض أساليب الحماية المتبعة من قبل العمادة ومن ذلك ما يلي:

أ. عدم تحديث برنامج الحماية ضد الفيروسات بشكل منتظم لخادم الشبكة وجميع محطات العمل مما أدى إلى تعرض بعض محطات العمل للإصابة بالفيروسات أكثر من مرة.

ب. تباعد الفترة الفاصلة بين كل نسخ احتياطي والنسخ التالي له مما يعرض بيانات (٣٩٥) تسجيلة فهرسة في المتوسط للفقدان خلال تلك الفترة، إلى جانب تسجيلات الإعارة المعرضة للفقدان في الفترة نفسها.

ج. عدم تحديد صلاحيات المستخدمين من الموظفين وفقاً لما يتطلبه عملهم الفعلي بالمكتبة.

د. ضبط إتاحة الوصول للشبكة وفقاً للموقع في قسم الإعارة بدلاً من ضبطه وفقاً للأشخاص.

ه. عدم تدريب موظفي المكتبة على التعامل مع المشكلات التي قد تواجههم والمتعلقة أمن المعلومات.

و. عدم مراعاة القواعد المتبعة لحماية كلمات المرور والتي تضمن عدم كشفها من قبل الآخرين.

ز. عدم الالتزام فعلياً بتطبيق بعض ما جاء في القواعد التنظيمية الصادرة عن مركز المعلومات والحاسب الآلي والتطوير الجامعي والمعتمدة من إدارة الجامعة

ولتطوير الأساليب المتبعة لحماية أمن شبكة المعلومات بالعمادة توصي الباحثة بالآتي:

١- اتباع بعض الإجراءات الأمنية اللازمة لإحكام أمن المعلومات خصوصاً في ظل ارتباط الشبكة المحلية بشبكة الإنترنت؛ ومن تلك الإجراءات تقنية الحوائط النارية والتشفير ودعم أجهزة عدم انقطاع التيار الكهربائي.

٢- تحديد صلاحيات المستخدمين بحيث لا يتاح لكل موظف ممارسة أي نشاط على قاعدة البيانات حتى لو كانت تلك النشاطات مرتبطة بالقسم الذي يعمل فيه الموظف سواء كان قسم الإجراءات الفنية أم قسم الإعارة أم غيرهما.

٣- التوثيق للمشكلات التي تعترض الشبكة والأساليب التي تم اتباعها لحلها وذلك حتى يمكن التغلب على تلك المشكلات بشكل سريع في حالة تكرار الوقوع فيها.

٤- الحرص على تحديث برنامج الحماية ضد الفيروسات بصورة منتظمة ومتقاربة لكل من خادم الشبكة ومحطات العمل.

٥- إلحاق بعض موظفي المكتبة بدورات تدريبية حول حماية أمن المعلومات على الشبكات.

٦- العمل فعلياً بما جاء في القواعد التنظيمية الصادرة عن مركز المعلومات والحاسب الآلي والتطوير الجامعي والمعتمدة من إدارة الجامعة.

قائمةالمراجع

1. ***Rowley J. Is your computer system secure? .- managing Information .- 2(7/8)Jul/Aug 1995.- p. 38-39***
2. ***Cerwone F . Security and the new ILLINET online system .- Illinois- Libraries .- 79(3) summer1997 .- p. 117-122***

٣. أشرف الغنيمي . نظم الحماية من قراصنة الكمبيوتر .- القاهرة: دار الفاروق للنشر والتوزيع، ١٩٩٨م .- ١٦٤ص

4. ***Hawkins S & Yen D.C & Chou D. C . Awareness and challenge of Internet security .- Information Management and Computer Security .- 8(2/3) 2000 .- p. 131-143***

٥. حسن طاهر داود. الحاسب وأمن المعلومات .- الرياض: معهد الإدارة العامة، ١٤٢١هـ/٢٠٠٠م .- ٤٣١ص

٦. دليل مصطلحات الحاسب: دليل المستخدم/ ترجمة عماد مصطفى.- حلب:شعاع للنشر والعلوم،١٩٩٤،ص٢٤٤

7. ***Christa Anderson & Mark Minasi . Mastering Local Area Networks .- San Francisco: SYBEX Network Press ,1999 .- p560***

٨. حسن طاهر داود. مرجع سابق .- ص٣٠٥-٣٠٩

9. ***Christa Anderson & Mark Minasi . op.cit.-p574***

١٠. مارك سبورتاك ، والتر غلين . علم نفسك ***MCSE*** أساسيات شبكات الاتصال.- بيروت: الدار العربية للعلوم،١٩٩٨م .-ص ٢٤٢-٢٤٤ ، و حسن طاهر داود. مرجع سابق .-ص ٤٥،٣٨-٣٣٢،٤٦

١١. سيد مصطفى أبو السعود .كيف تصبح مديراً لشبكة الكمبيوتر .- القاهرة: دار الكتب العلمية، ٢٠٠٠م .- ص٣٦٧-٣٧١

12. ***Lyn Robinson .Installing a Local Area Network .- London: Aslib , 1995 .-p36***

و مارك سبورتاك ، والتر غلين . مرجع سابق .-ص٢٤٤-٢٤٥

13. ***Christa Anderson & Mark Minasi . op.cit.-p. 562-563***
14. ***Ibid. .-p565,665-666***

١٥. مارك سبورتاك ، والتر غلين . مرجع سابق .-ص٢٤٥-٢٤٦

16. *Christa Anderson & Mark Minasi . op.cit..-p578*

17. *Patrik Grote . Network+ Cheat Sheet .- Indianapolis: Que corporation, 2000.- p175*

١٨. تركي بن أحمد العصيمي . احم جهازك المخاطر الأمنية وطرق الحماية منها .- الرياض: دار المعارج، ١٤٢٠هـ.- ص١٨٨-١٨٩

19. *Christa Anderson & Mark Minasi . op.cit.- 571-574*

٢٠. حسن طاهر داود. مرجع سابق .- ص١٧٩-١٩٠، ٢٠٢-٢٠٣

21. *Glossary of messaging and network security Terms.- http://www.ssimail.com/Glossary.htm. [1/3/01]*

٢٢. تركي بن أحمد العصيمي . مرجع سابق .-ص ٢٣٦

٢٣. حسن طاهر داود. مرجع سابق .-ص٣٦٨

24. *Patrik Grote . op.cit .- p176*

٢٥. أشرف الغنيمي . مرجع سابق .- ص ١٥٠

٢٦. تركي بن أحمد العصيمي . مرجع سابق .- ص٢٠٢-٢٠٦

٢٧. دودج لوي . الشبكات للمبتدئين .- الرياض: مكتبة جرير، ١٩٩٨م .-ص ٢٤٠

٢٨. أشرف الغنيمي . مرجع سابق .- ص ٢٩-٣٢ و *Glossary of messaging and network security Terms .-op.cit*

٢٩. دليل مصطلحات الحاسب : دليل المستخدم . مرجع سابق .- ص٤٤٦، و تركي بن أحمد العصيمي . مرجع سابق.- ص٨٣،٢١٦-٢١٧ ، و الحاسب وأمن المعلومات .-ص٧٧ و تركي بن أحمد العصيمي . مرجع سابق .- ص٢١٥-٢١٦، و أشرف الغنيمي . مرجع سابق .-ص٥٣

٣٠. مارك سبورتاك ، والتر غلين . مرجع سابق .-ص٢٤٩

31. *Patrik Grote . op.cit.- p202*

٣٢. حسن طاهر داود. مرجع سابق .- ص ٢٤٢-٢٤٤

٣٣. مارك سبورتاك ، والتر غلين. مرجع سابق .-ص٣٢٠-٢٥٠،٣٢٢-٢٥١

٣٤. دودج لوي. مرجع سابق .-ص٢٣٠-٢٣١، وسيد مصطفى أبو السعود .- مرجع سابق .-ص٣٧٥، و مارك سبورتاك ، والتر غلين . مرجع سابق .-ص٢٥١

٣٥. جايمس سيميك . ***Microsoft MCSE*** الاستعداد الأقصى للامتحان ***10-058*** أساسيات شبكات الاتصال .- بيروت: الدار العربية للعلوم، ١٩٩٩م .-ص ٢٤٣، و مارك سبورتاك ، والتر غلين. مرجع سابق .-ص٢٥٠

٣٦. مارك سبورتاك ، والتر غلين. مرجع سابق .-ص٢٥٠

٣٧. أشرف الغنيمي . مرجع سابق .- ص ١٣١-١٣٦ ، ١٣٩-١٤٠، و حسن طاهر داود. مرجع سابق.- ص٥٠-٥١

38. Christa Anderson & Mark Minasi . op.cit .- p559

٣٩. البرامج الخدمية المضادة للفيروسات .- ***PC Magazine***.- الطبعة العربيـــة .- س٣، ع٧ (يوليو/أغسطس ١٩٩٧) .- ص٥٦-٦٢

٤٠. حلول جديدة للفيروسات .- ***PC Magazine*** .- الطبعة العربية .- س٤، ع٢ (فبراير ١٩٩٨) .- ص ٢١ و برنامج كشف إزالة الفيروسات نورتن أنتي فيروس ديلـــوكس ***4.0*** .- ***PC Magazine*** .- الطبعة العربية .- س٤، ع٣ (مارس ١٩٩٨) .- ص٤٦

ملحق ١

١. هل تخصص غرفة مستقلة لحفظ أجهزة الخادم

( ) نعم ( ) لا

- في حالة الإجابة بلا .. فأين يتم وضعها:

( ) مع مكاتب الموظفين

( ) في مكان استخدام المستفيدين

( ) في موقع آخر .. الرجاء تحديده ...

٢. هل تستخدم تقنية الحوائط النارية ***firewalls*** لحماية الشبكة

( ) نعم ( ) لا

- في حالة الإجابة بلا .. فالرجاء الانتقال الى سؤال رقم ٥

٣. هل تستخدم تقنية الحوائط النارية لديكم:

( ) برنامج فقط

( ) برنامج مع أجهزة

٤. ما التقنية المستخدمة لديكم

( ) ***McAfee Firewalls***

( ) ***Guardian NT firewall***

( ) أخرى .. الرجاء تحديدها...

٥. هل تستخدم برنامج حماية ضد الفيروسات

( ) نعم ( ) لا

- في حالة الإجابة بنعم ..فما البرنامج المستخدم لديكم:

( ) ***McAfee***

( ) ***Norton AntiVirus***

( ) آخر .. الرجاء تحديده ...

٦. هل تعمل المكتبة نسخاً احتياطية للملفات.

( ) نعم ( ) لا

-في حالة الإجابة بلا .. فالرجاء الانتقال الى سؤال رقم ١٣

٧. هل يتم النسخ الاحتياطي على فترات منتظمة

( ) نعم ( ) لا

- في حالة الإجابة بنعم .. الرجاء تحديد الفترة ...

٨. ما نوع النسخ الذي تقوم به المكتبة

( ) نسخ كامل لكافة الملفات والبرامج ***full backup***

( ) نسخ تراكمي ***incremental backup***

( ) نسخ تفاضلي ***differential backup***

( ) طريقة أخرى .. الرجاء تحديدها

٩. ما البيانات التي يتم نسخها احتياطياً

( ) الملف الخاص بالمستخدمين وحقوقهم وكلمات المرور الخاصة بهم

( ) البريد الإلكتروني

( ) قواعد البيانات

( ) أخرى .. الرجاء تحديدها ...

١٠. على أي وسيط يتم النسخ الاحتياطي

( ) أقراص مرنة

( ) أقراص صلبة

( ) وسيط آخر .. الرجاء تحديده ...

١١. كم عدد النسخ الاحتياطية التي تحتفظ بها المكتبة

( ) نسخة واحدة

( ) نسختان

( ) عدد آخر .. الرجاء تحديده

١٢. أين يتم حفظ النسخ الاحتياطية

( ) داخل المكتبة

( ) خارج المكتبة.. الرجاء التحديد...

( ) بعضها داخل المكتبة والبعض خارجها

١٣. هل تحدد المكتبة كلمات عبور ***password*** لمستخدمي الشبكة

( ) نعم ( ) لا

-في حالة الإجابة بلا ..فالرجاء الانتقال الى سؤال رقم ١٧

١٤. على أي أساس تحدد كلمات العبور

( ) على أساس المستخدم

( ) على أساس الموقع

١٥. هل يتم تغيير كلمات المرور كل فترة

( ) نعم ( ) لا

- في حالة الإجابة بنعم .. الرجاء تحديد مدة استخدام كلمة المرور...

١٦. ما الذي يميز كلمات المرور التي يتم اختيارها عادة

( ) طويلة ولا تقل عن ٨ محارف

( ) قصيرة وسهلة التذكر

( ) تتكون من حروف فقط

( ) تتكون من حروف وأرقام

( ) تتكون من حروف وأرقام ورموز

( ) مرتبطة بعبارات مستخدمة في المكتبة

( ) غير ذلك .. الرجاء التحديد ...

١٧. ما المشكلات الأمنية التي تعرضت لها الشبكة من قبل

( ) اقتحام بعض المستخدمين غير المصرح لهم بالاستخدام

( ) تعرض البيانات للتلف أو الفقدان نتيجة لعوامل طبيعية

( ) تعرض البيانات للتلف أو الفقدان نتيجة سوء استخدام الموظفين

( ) تعرض البيانات للتلف أو الفقدان نتيجة لتعرض الشبكة للفيروسات

( ) مشكلات أخرى .. الرجاء تحديدها...

١٨. كيف تمت معالجة تلك المشكلات

( ) تمت إحالة الجهاز الى جهة الاختصاص بالجامعة لحل المشكلة

( ) تم استدعاء الشخص المختص من خارج العمادة لحل المشكلة

( ) تم استدعاء الشخص المختص من داخل العمادة لحل المشكلة

( ) طريقة أخرى .. الرجاء تحديدها...

١٩. هل تم تدريب موظفي المكتبة على كيفية التعامل مع المشكلات التي تواجههم

( ) نعم ( ) لا

في حالة الإجابة بلا .. فهل يرجع السبب إلى

( ) وجود متخصصين في صيانة الشبكات في المكتبة

( ) وجود متخصصين في صيانة الشبكات في الجامعة

( ) أسباب أخرى .. الرجاء تحديدها ...

٢٠. هل توثق المكتبة المشكلات التي تعترض الشبكة وطرق حلها

( ) نعم ( ) لا

٢١. الرجاء ذكر أي معلومات أخرى مرتبطة بأمن شبكة المكتبة في المساحة المتبقية من الصفحة....